SuperStack® 3
Firewall
User Guide

SuperStack 3 Firewall 3CR16110-95
SuperStack 3 Firewall Web Site Filter 3C16111

http://www.3com.com/

Part No. DUA1611-0AAA02
Published August 2001

3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

3Com Technologies reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Technologies to provide notification of such revision or change.

3Com Technologies provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and SuperStack are registered trademarks of 3Com Corporation. The 3Com logo and CoreBuilder are trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Netscape Navigator is a registered trademark of Netscape Communications.

JavaScript is a trademark of Sun Microsystems

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

CONTENTS

ABOUT THIS GUIDE

I GETTING STARTED

1 INTRODUCTION

2 INSTALLING THE HARDWARE

3 Quick Setup for the Firewall

II Configuring the Firewall

4 Basic Settings of the Firewall

12 TROUBLESHOOTING GUIDE

IV FIREWALL AND NETWORKING CONCEPTS

13 TYPES OF ATTACK AND FIREWALL DEFENCES

ABOUT THIS GUIDE

This guide describes the following products:

- SuperStack 3 Firewall 3CR16110-95
- SuperStack 3 Firewall 3CR16110-97 upgraded to v6.x firmware
- SuperStack 3 Firewall Web Site Filter 3C16111

Introduction

This guide describes how to set up and maintain the SuperStack® 3 Firewall and how to install and use the SuperStack 3 Web Site Filter.

The Firewall acts as a secure barrier to protect a private LAN from hacker attacks from the Internet. It can also be used to control the access that LAN users have to the Internet.

The Web Site Filter controls and monitors the access users have to web sites. Sites can be blocked on a site-wide or individual basis and by the features a web site uses or content it provides.

This guide is intended for use by the person responsible for installing or managing the network. It assumes knowledge of the following:

- Basic familiarity with Ethernet networks and the Internet Protocol.
- Knowledge of how to install and handle electronically sensitive equipment.

If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

`http://www.3com.com/`

How to Use This Guide

Table 1 shows where to look for specific information in this guide.

Table 1 Where to find specific information

If you are looking for...	Turn to...
A description of the Firewall's features and example applications.	Chapter 1
A description of the Firewall's front and back panel displays and connectors, and installation information.	Chapter 2
A quick setup guide for the Firewall.	Chapter 3
Information on how to configure the Firewall.	Chapter 4 - Chapter 10
Information about installing and setting up the Web Site Filter.	Chapter 11
Troubleshooting common Firewall problems.	Chapter 12
Information about Denial of Service and other attacks.	Chapter 13
An introduction to TCP/IP and VPN.	Chapter 14
Important Safety Information.	Appendix A
Technical Specifications of the Firewall.	Appendix B
Cable Specifications.	Appendix C
Information about obtaining Technical Support.	Appendix D

Conventions

Table 2 and Table 3 list conventions that are used throughout this guide.

Table 2 Notice Icons

Icon	Notice Type	Description
i	Information note	Information that describes important features or instructions.
⚠	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
⚡	Warning	Information that alerts you to potential personal injury.

Table 3 Text Conventions

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
`Commands`	The word "command" means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold. Example: To display port information, enter the following command: **`bridge port detail`**
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

Terminology

This section lists terminology used in this guide.

DMZ — Demilitarized Zone port. The Firewall has an extra port. If you connect publicly-accessible servers and workstations to this port, they are accessible from the Internet but still protected from Denial of Service attacks

DoS Attacks — Denial of Service Attacks. An attempt to stop one of your services running, such as a Web or FTP server. There are several kinds of DoS attacks.

IP address — The Internet Protocol address is the network layer address of a device assigned by the user or network administrator of an IP network. An IP address consists of 32 bits divided into two or three fields:

a network number and a host number, or a network number, a subnet number, and a host number.

IP Spoof — A type of DoS attack. An IP spoof uses a fake IP address to bypass security settings which may bar access from the real IP address.

IRC — Internet Relay Chat. Provides a way of communicating in real time with people from all over the world.

ISP — Internet Service Provider. A business that provides Internet access to individuals or organizations.

Firewall — Used in this guide to refer to the SuperStack 3 Firewall.

Land Attack — A type of DoS attack. In a Land attack, a packet is sent that appears to come from the same address and port that it is sent to. This can hang the machine to which it is sent.

Management Station — This is the workstation from which you run the Web interface for the Firewall.

Web interface — This is the Web-based application which you use to set up the Firewall to protect your network from attack and to control access to the Internet for LAN users.

NAT — Network Address Translation. NAT refers to the process of converting the IP addresses used within a private network to Internet IP addresses.

NTP — Network Time Protocol. This allows the Firewall to automatically set the local time, via an NTP server on the Internet

NNTP — Network News Transfer Protocol. This protocol is used to distribute Usenet news articles over the Internet.

Ping of Death — A type of DoS attack. The Internet Protocol (IP) defines the maximum size for a Ping packet. However, some Ping programs can send packets that are larger than this size which can cause some systems to crash.

PPPoE — PPPoE stands for Point-to-Point Protocol over Ethernet and is based on two widely accepted standards, Point-to-Point Protocol (PPP) and Ethernet. PPPoE is a method for personal computers to connect to a broadband service (typically DSL).

RADIUS — Remote Authentication Dial-in User Service. RADIUS enables network administrators to effectively deploy and manage VPN Client based remote users. The RADIUS server allows multiple users to share a single Group Security Association but require an additional unique password for accounting and access.

SYN Flood — A type of DoS attack. This is where a client opens a connection with a server but does not complete it. If the server queue fills up with partially-open connections, no other clients can make genuine connections to that server.

UTC —stands for Universal Time Co-ordinated, and is the standard time common to all places in the world. It is also commonly referred to as GMT or World Time.

VPN — stands for Virtual Private Network, and is a method of networking that uses data encryption and the public internet to provide secure communications between sites without incurring the expense of leased lines.

Web Site Filter — Used in this guide to refer to the SuperStack 3 Web Site Filter.

See Chapter 13, "Types of Attack and Firewall Defences" for further information on types of attack and how the Firewall defends against them.

Feedback about this User Guide

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when commenting:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- SuperStack 3 Firewall User Guide

- Part Number DUA1611-0AAA02
- Page 24

Do not use this e-mail address for technical support questions. For information about contacting Technical Support, see Appendix A.

Registration

To register your Firewall point your web browser to

`http://www.3com.com/ssfirewall`

click on *Hardware Registration* and follow the instructions.

I GETTING STARTED

1 INTRODUCTION

This chapter contains the following:

- What is the SuperStack 3 Firewall?
- Firewall and 3Com Network Supervisor
- Firewall Features
- Introduction to Virtual Private Networking (VPN)

What is the SuperStack 3 Firewall?

The SuperStack® 3 Firewall is a dedicated firewall appliance which is installed between a Private LAN and a Router. The Firewall is a complete network security system with all hardware and software pre-installed. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The purpose of the Firewall is to allow a private Local Area Network (LAN) to be securely connected to the Internet. You can use the Firewall to:

- Prevent theft, destruction, and modification of data.
- Filter incoming data for unsafe or objectionable content.
- Log events which may be important to the security of your network.

The Firewall has three Ethernet ports which are used to divide the network into separate areas.

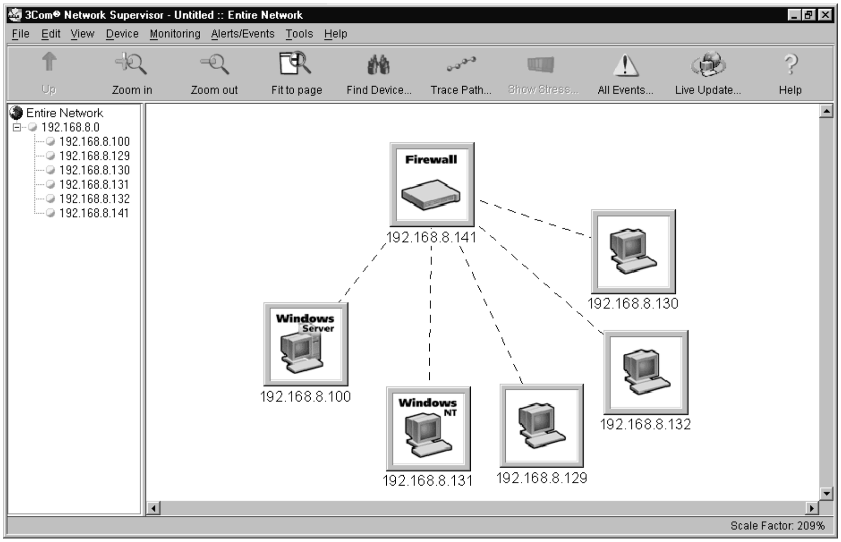
- The *Wide Area Network* (WAN) port attaches to the Internet access device, for example, Router or Cable Modem.
- The *Local Area Network* (LAN) port attaches to the local network through hubs and switches. LAN users have access to Internet services such as e-mail, FTP, and the World Wide Web. However, all workstations and data on the LAN are protected from hacker attacks that might come through the WAN port.

- The *Demilitarized Zone* (DMZ) port is used for public servers, such as Web or FTP servers. Machines attached to this port are visible from the WAN port, but are still protected from hacker attacks. Users on the secure LAN port can also access servers on the DMZ port.

Firewall and 3Com Network Supervisor

The Firewall is supplied with a copy of 3Com Network Supervisor. Network Supervisor is a powerful, intuitive network management application for small to medium enterprise networks.

Figure 1 3Com Network Supervisor display



Network Supervisor automatically discovers up to 1500 network devices and shows devices and connections on a graphical display. Network managers can view network activity, monitor stress and set thresholds and alerts. This information helps to provide the most efficient, cost-effective use of network resources.

Version 3.0 and later releases add significant extra functionality designed to detect network inefficiency and optimize network performance. Features include support for related and recurring events, user definable reports, auto-alerting using pager or SMS messages and simple updates from the 3Com web site.

3Com Network Supervisor offers the following support to Firewall users:

- If your 3Com Network Supervisor management station is located on the LAN, it discovers the Firewall automatically and displays it on the topology map.
- The topology map indicates that the Firewall is a 3Com Firewall and uses an appropriate icon to represent it.
- Double-clicking on the Firewall icon launches the Web interface of the Firewall.

If your 3Com Network Supervisor management station is located on the WAN side of the Firewall you must follow the steps below before Network Supervisor will detect your Firewall:

1. Access the Web interface from a Web browser connected to the LAN port of the Firewall.
2. Click on the *Policy* button, after the Management screen appears.
3. Click on the *User Privileges* tab.
4. Add a user to the *Current Privileges* list. Enter the user name in the *User* field.
5. Click on *Remote Access* and click *Update Privileges*.

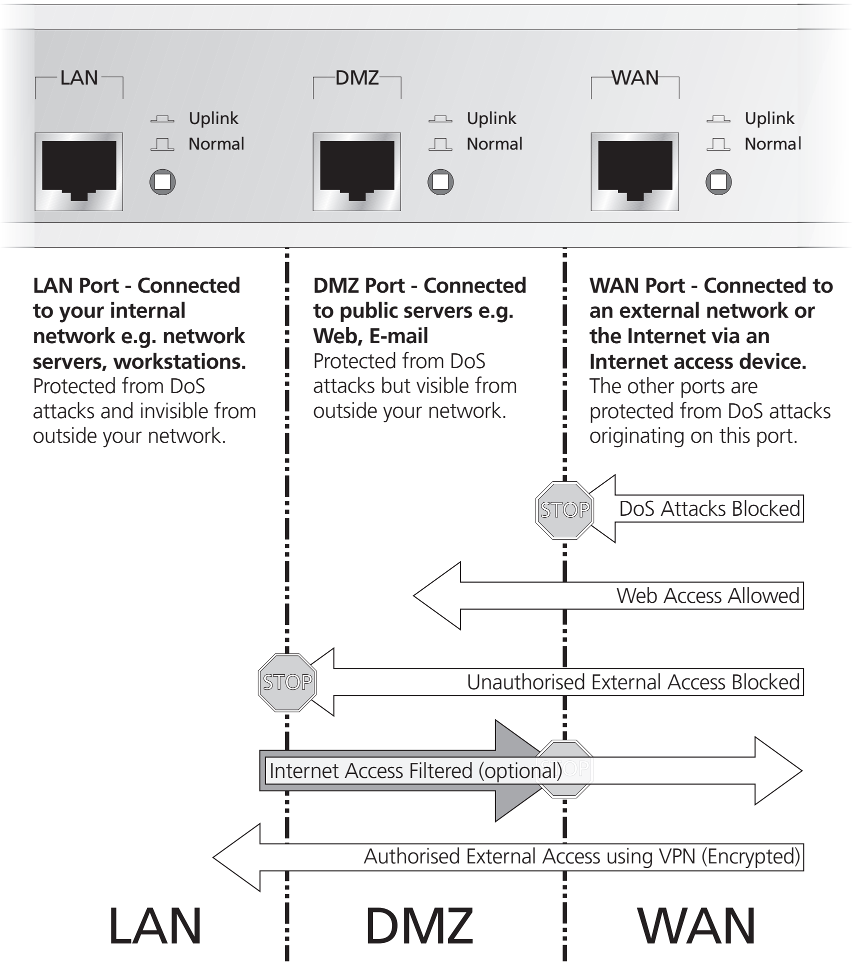
Firewall Features

This section lists the features of the Firewall.

Firewall Security

The Firewall is preconfigured to monitor Internet traffic, and detect and block *Denial of Service* (*DoS*) hacker attacks automatically. Refer to Figure 2.

Figure 2 Firewall Security Functions - Default Firewall Policy


LAN
Uplink
Normal
DMZ
Uplink
Normal
WAN
Uplink
Normal
LAN Port - Connected to your internal network e.g. network servers, workstations. Protected from DoS attacks and invisible from outside your network.
DMZ Port - Connected to public servers e.g. Web, E-mail Protected from DoS attacks but visible from outside your network.
WAN Port - Connected to an external network or the Internet via an Internet access device. The other ports are protected from DoS attacks originating on this port.
STOP
DoS Attacks Blocked
Web Access Allowed
STOP
Unauthorised External Access Blocked
Internet Access Filtered (optional)
Authorised External Access using VPN (Encrypted)
LAN
DMZ
WAN

The Firewall examines every packet that comes from outside the LAN and discards any packet that has not been authorized from inside the LAN. This is known as stateful packet inspection.

Users on the LAN have access to all resources on the Internet that are not blocked by any of the filters.

Users on the Internet can access hosts on the DMZ, such as a Web server, but cannot access any resources on the LAN unless they are authorized remote users.

The Firewall will protect your network against the following Denial of Service attacks:

- Ping of Death
- Smurf Attack
- SYN Flood
- LAND Attack
- IP Spoofing
- Teardrop

To find more information on DoS and other attacks refer to Chapter 13, "Types of Attack and Firewall Defences"

Advanced users can extend the security functions of the Firewall by adding network access rules and user privileges. See "Examples of Network Access Rules" on page 200 and "User Privileges" on page 205 for more information.

Web URL Filtering

You can use the Firewall to monitor and restrict LAN users from accessing inappropriate information on the Internet. You can block access to this information or record attempts to access it in a log. See "Filter Settings" on page 162 for more information.

You can create a list of all *forbidden* URLs to which you want to restrict access. Alternatively, you can restrict access to the Internet to certain *trusted* URLs. See "Setting up Trusted and Forbidden Domains" on page 165 for more information.

Web site technologies such as cookies and Java and ActiveX applets give enhancements to web pages, but hackers may use the technologies to steal or damage data. The Firewall can block these potentially damaging applications from being downloaded from the Internet, or allow them only from trusted sites. See "Filter Settings" on page 162 for more information.

You can also use the optional SuperStack 3 Web Site Filter to extend these filtering capabilities of your Firewall. It provides a list of Web site categories that might be considered inappropriate for business use. The Web Site Filter updates the Firewall with the latest URLs matching the selected categories. You can block access to these sites or log them. The Firewall is supplied with a one-month free subscription. You can then purchase a twelve month Web Site Filter (3C16111) subscription. Both the trial and the twelve month subscription are valid for an unlimited number of users.

High Availability

Given the mission critical nature of many Internet connections each component involved in your connection must be highly reliable. The *High Availability* function of your Firewall adds to the already reliable platform eliminating downtime due to hardware failure.

To use the *High Availability* function, connect another SuperStack 3 Firewall to the first as a high availability pair and configure the backup Firewall to monitor the primary Firewall. In the event of failure of the primary Firewall, the backup Firewall will take over its functions. See "Configuring High Availability" on page 141 for details.

Logs and Alerts

The Firewall maintains a log of all events that could be seen as security concerns. It can also track key events such as the top 25 most accessed Web sites, or the top 25 users of Internet bandwidth. You can also set up the Firewall to send an alert message through e-mail when a high-priority concern, such as a hacker attack, is detected. See "Log/Alert Settings" on page 177 for more information.

For detailed logging 3Com recommends that you us a syslog server or a syslog reporting tool. A free syslog server is available from 3Com. To download it point your web browser to:

```
http://www.3com.com/ssfirewall
```

and follow the link to the *Syslog Server*.

User Remote Access (from the Internet)

Users can access intranet resources on the private LAN by successfully logging into the Firewall from the Internet. Logging in requires a valid user name and password, which are transmitted to the Firewall by the remote user, using a Web browser, through an MD5-based encrypted authentication mechanism. Once logged in, remote users are able to access all IP resources on the LAN

Automatic IP Address Sharing and Configuration

The Firewall provides sharing of a single public IP address through *Network Address Translation* (*NAT*). It also provides simplified IP address administration using the *Dynamic Host Configuration Protocol* (*DHCP*).

NAT automatically translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. It enables the Firewall to be used with broadband modems such as the OfficeConnect Cable Modem, and with low cost Internet accounts where only one IP address is provided by the ISP. See "Network Addressing Mode" on page 149 for more information.

The DHCP server automatically assigns all PCs on the LAN with the correct IP information. The DHCP client allows the Firewall to acquire the correct IP settings from the ISP. See "Setting up the DHCP Server" on page 155 for more information.

Introduction to Virtual Private Networking (VPN)

The Firewall includes support for IPSec Virtual Private Networking. This section provides an introduction to Virtual Private Networking (VPN).

Virtual Private Networking

Today's business environment requires close, real-time collaboration with trading partners, legal, and financial advisors, as well as remote workers and branch offices. This "real-time" requirement often leads to the creation of an "extranet" where branch offices and partners are connected to a primary network in one of two ways:

- Leasing dedicated data lines to connect all sites.
- Using the public Internet to connect all sites and remote users together.

Each of these methods has its benefits and drawbacks. Establishing a leased line connection between the sites offers a dedicated, secure access but at a very high cost.

The other option is to use an existing Internet connection to transmit data unencrypted over the public Internet network. While this option is less expensive and can provide higher performance, it is much less secure than dedicated site-leased lines.

VPN uses data encryption and the public Internet to provide secure communications between sites without incurring the huge expense of site to site leased lines.

The Firewall embodies eight different levels of encryption that can be used to create a VPN tunnel. For the tunnel to work correctly, the terminating device at the other end of the tunnel must be using the same level and type of encryption. See "Configuring Virtual Private Network Services" on page 123 for more details.

2 INSTALLING THE HARDWARE

This chapter contains the following:

- Before You Start
- Positioning the Firewall
- Firewall Front Panel
- Firewall Rear Panel
- Redundant Power System (RPS)
- Attaching the Firewall to the Network

⚠ ***WARNING:*** *Before installing the Firewall, you must read the safety information provided in Appendix A of this User Guide.*

⚠ ***AVERTISSEMENT:*** *Avant d'installer le Firewall, lisez les informations relatives à la sécurité qui se trouvent dans l'Appendice A de ce guide.*

⚠ ***VORSICHT:*** *Bevor Sie den Firewall hinzufügen, lesen Sie die Sicherheitsanweisungen, die in Anhang A in diesem Handbuch aufgeführt sind.*

Before You Start

Your SuperStack 3 Firewall (3CR-15110-95) comes with the following:

- A power cord for use with the Firewall.
- Four rubber feet.
- Mounting Kit for a 19 in. rack mount cabinet comprising:
  - two mounting brackets.
  - four screws.
- A SuperStack 3 Firewall User Guide (this guide).
- A SuperStack 3 Firewall Quick Reference Guide (DQA1611-0AAA01)

- A SuperStack 3 Firewall CD.
- Warranty Information.
- Software License Agreement.

Positioning the Firewall

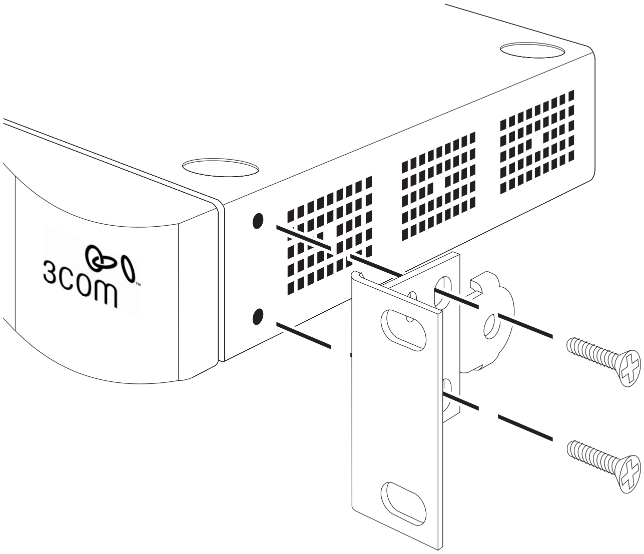
When installing the Firewall, make sure that:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radio transmitters and broadband amplifiers.
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted. 3Com recommends that you provide a minimum of 25.4 mm (1 in.) clearance to each side of the unit.

Rack Mounting the Units

The Firewall is 1U high and will fit a standard 19-inch rack.

Figure 3 Fitting the Rack Mounting Bracket



***CAUTION:** Disconnect all cables from the unit before continuing. Remove the self-adhesive pads from the underside of unit, if already fitted.*

1. Place the unit the right way up on a hard, flat surface with the front facing towards you.
2. Locate a mounting bracket over the mounting holes on one side of the unit (refer to Figure 3).
3. Insert the two screws supplied in the mounting kit and fully tighten with a suitable screwdriver.
4. Repeat the steps 2 and 3 for the other side of the unit.
5. Insert the unit into the 19-inch rack and secure with suitable screws (not provided).
6. Reconnect all cables.

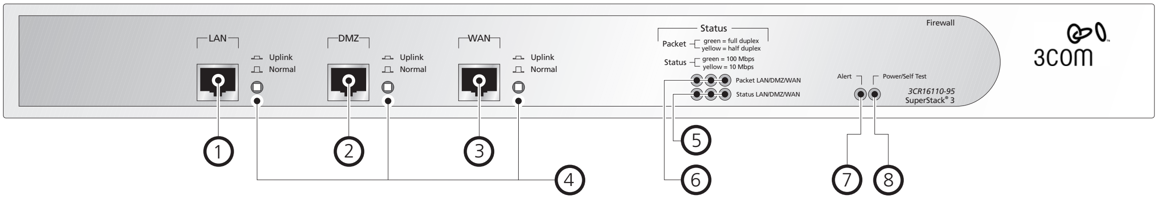
Securing the Firewall with the Rubber Feet

The four self-adhesive rubber feet prevent the Firewall from moving around on the desk. Only stick the feet to the marked areas at each corner of the underside of the unit if you intend to place the unit directly on top of the desk.

Firewall Front Panel

Figure 4 shows the front panel of the Firewall.

Figure 4 Firewall Front Panel



***WARNING:** RJ-45 Ports. These are shielded RJ-45 data sockets. They cannot be used as standard traditional telephone sockets, or to connect the unit to a traditional PBX or public telephone network. Only connect RJ-45 data connectors, network telephony systems, or network telephones to these sockets.*
Either shielded or unshielded data cables with shielded or unshielded jacks can be connected to these data sockets.

The Firewall front panel contains the following components:

1 **LAN Port** - Use a Category 5 cable with RJ-45 connectors. Connect this port to any workstation or network device that has a 10BASE-T or 100BASE-TX port.

2 **DMZ Port** - Use a Category 5 cable with RJ-45 connectors. Use this port to connect the Firewall to any workstation, server, or network device that has a 10BASE-T or 100BASE-TX port.

3 **WAN Port** - Use a Category 5 cable with RJ-45 connectors. Connect this port to any Internet access device that has a 10BASE-T or 100BASE-TX port.

4 **Normal/Uplink Switches** - The setting of these switches determines the operation of each port. See "Attaching the Firewall to the Network" on page 32 for more information about setting these switches.

5 **Status LEDs** - The WAN, LAN, and DMZ ports each have a Status LED that indicates the following:

- *Green* indicates that the link between port and the next network device is operational at 100 Mbps.
- *Yellow* indicates that the link between the port and the next network device is operational at 10 Mbps.
- *Off* indicates that nothing is operational or that the link to the port has failed.

6 **Packet LEDs** - The WAN, LAN, and DMZ ports each have a Packet LED that indicates the following:

- *Green* indicates that data is being transmitted/received on this port in full-duplex mode.
- *Yellow* indicates that data is being transmitted/received on this port in half-duplex mode.
- *Off* indicates that no traffic is being passed.

7 **Alert LED** - This LED shows orange to alert you of the following:

- A failure in the self-test the Firewall runs when switched on.
- No operational firmware is currently loaded.
- Potential attacks on your network.
- An attempt to access a restricted site.
- A hacker attack or access to a restricted service.

To diagnose faults see "Troubleshooting Guide" on page 167.

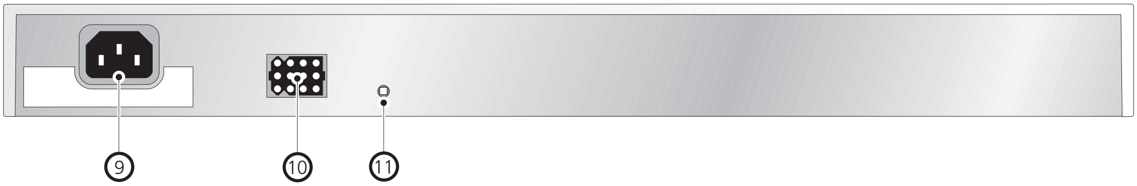
8 **Power/Self Test LED** - This LED shows green to indicate that the unit is switched on. This LED flashes for about 90 seconds while self-test is running, and also when restarting.

If you have installed a 3Com RPS unit with the Firewall and the RPS has a fault, the Power LED will flash to warn you. Once the fault on the RPS has been rectified, the Power LED will stop flashing.

Firewall Rear Panel

Figure 5 shows the rear panel of the Firewall.

Figure 5 Firewall Rear Panel



The Firewall rear panel contains the following components:

9 **Power socket** - Only use the power cord supplied with the Firewall.

10 **Redundant Power System socket** - Use this connector to attach a Redundant Power System to the Firewall.

11 **Reset Switch** (recessed) - Use to reset the Firewall.

⚠ ***CAUTION:*** *Holding the Reset Switch when you power on the Firewall will erase the operational firmware and return the device to factory default settings. To reset the Firewall see "Restore Factory Defaults" on page 187.*

Redundant Power System (RPS)

The SuperStack 3 Advanced Redundant Power System (RPS) offers you the flexibility to supply power to your SuperStack devices in the event of a failure of an internal power supply. The System is a group of products from which you choose the most suitable for your equipment and its configuration. One RPS unit can supply up to eight SuperStack 3 units.

The RPS status is displayed in the *Unit Status* screen on the Web interface.

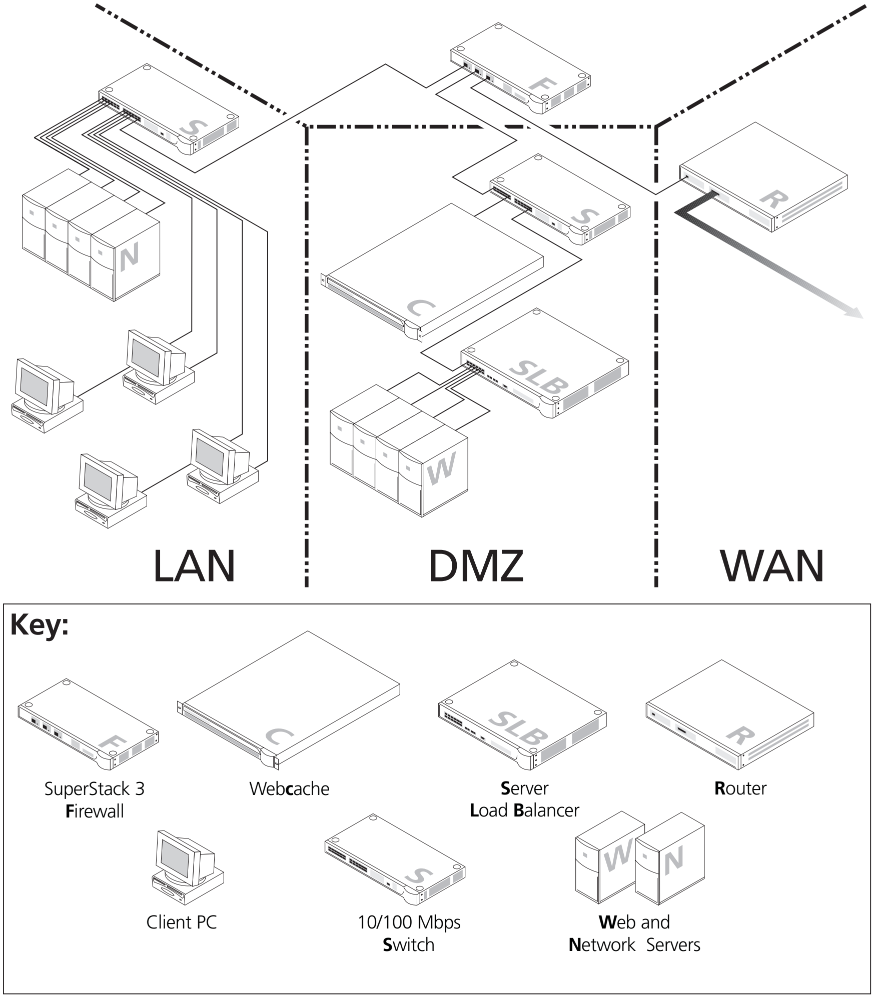
Use the following SuperStack 3 RPS with the Firewall:

- SuperStack 3 - Advanced RPS (3C16071)
- and 60W RPS Power Module - (3C16072)

Attaching the Firewall to the Network

Figure 6 illustrates one possible network configuration.

Figure 6 Network Connection Diagram Showing Sample Network



Never connect two ports on the Firewall to the same physical network. For example, never connect the LAN and DMZ ports into the same device as this bypasses all firewall functions.

To attach the Firewall to your network:

1 Connect the Ethernet port labeled WAN on the front of the Firewall to the Ethernet port on the Internet access device.

Refer to the documentation for the Internet access device to find out the configuration of its Ethernet port. If it has an MDIX (normal) configuration, then you can use a standard Category 5 cable.

Make sure that the Uplink/Normal switch is in the **Uplink** position for a standard CAT-5 cable. If you are connecting the WAN port to a hub or switch with a crossover cable, or directly to a workstation with standard cable, make sure the Uplink/Normal switch is in the **Normal** position.

2 Connect the Ethernet port labeled LAN to your LAN.

If you are connecting the LAN port to a hub or switch using a standard Category 5 UTP cable, make sure that the Uplink/Normal switch for the LAN port is in the **Uplink** position. If you are connecting the LAN port to a hub or switch with a crossover cable, or directly to a workstation with standard cable, make sure the Uplink/Normal switch is in the **Normal** position.

3 Connect the Ethernet port labeled DMZ to the public servers.

If you are installing the Firewall DMZ and want to protect the public servers, such as Web and FTP servers, use the DMZ port. If you are connecting the DMZ port directly to a server using standard Category 5 cable, make sure that the Uplink/Normal switch is in the **Normal** position. If you are connecting the DMZ port to an Internet access device using standard Category 5 cable, make sure that the Uplink/Normal switch is in the **Uplink** position.

4 Turn on or restart the Internet access device.

5 Plug the Firewall into an AC power outlet, and then plug the power supply output cable into the power adapter socket.

6 Wait for the Power LED to stop flashing.

The Firewall is designed to start up as soon as power is supplied to it. Then it runs a series of self-diagnostics to check for proper operation. During these diagnostics, which take about 90 seconds, the Power LED flashes.

CAUTION: *Do not switch the Firewall off and on quickly. After switching it off, wait approximately five seconds before switching it on again.*

7 Make sure that the Link LEDs are on for all ports that are connected. If not, see Chapter 12 for troubleshooting information.

The Firewall is now attached to the network.

By default, no traffic that originates from the Internet is allowed onto the LAN, and all communications from the LAN to the Internet are allowed. That is, all inbound connections are blocked and all outbound connections are allowed.

You can now configure the Firewall. See the following chapters for more information:

- Chapter 3 for a quick setup guide for the Firewall.
- Chapters 4 to 8 for full information about all the configuration options.
- Chapter 11 for information about the Web Site Filter and Network Access Policy Rules.

At frequent intervals, check the Firewall for the following:

- The Alert LED is not continuously lit — if it is, there are problems on your network.
- The case vents are not obstructed.
- The cabling is secure and is not pulled taut.

3 QUICK SETUP FOR THE FIREWALL

This chapter contains the following:

- Introduction
- Setting up a Management Station
- Configuring Basic Settings
- Configuring WAN Settings
- Configuring LAN Settings
- Confirming Firewall Settings

Introduction

The first time the Firewall is started it runs an *Installation Wizard*. The Installation Wizard asks you questions about your network and configures the Firewall so that it works in your network.

If you later move your Firewall to another network and want to use the Installation Wizard to configure the Firewall you can activate the Installation Wizard manually. To start the Installation Wizard manually, click on the Tools menu, followed by the Configuration tab, then the Wizard button.

The configuration process can be split into three steps

1. To access the Installation Wizard you must first configure a computer as a *Management Station*. See “Setting up a Management Station” page 36 for details.
2. Launch a web browser on the Management Station and enter **`http://192.168.1.254`** to browse the Firewall.
3. Follow the instructions supplied by the Installation Wizard and answer the questions it asks.

The process followed by the Installation Wizard is described in the following sections:

- Configuring Basic Settings
- Configuring WAN Settings
- Configuring LAN Settings
- Confirming Firewall Settings

Setting up a Management Station

The Firewall has the following default settings:

- IP address — 192.168.1.254
- Subnet mask — 255.255.255.0

To access the Installation Wizard you must configure a computer to be in the same subnet. This computer will be referred to as a Management Station.

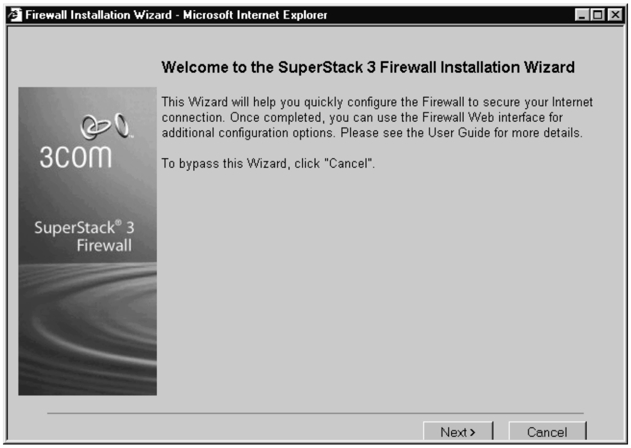
Follow the steps below to configure a computer as a Management Station:

1. Note the IP address and subnet mask of the Management Station. You will need to return your Management Station to these settings when you have finished using the Installation Wizard.
2. Change the IP address to a value within the Firewall's default subnet. This will be a value between `192.168.1.1` and `192.168.1.254` but not `192.168.1.254` as this is already taken by the Firewall. A suitable address would be `192.168.1.20` if this is not already taken by another device.
3. Enter `http://192.168.1.254/` (the Firewall's default IP address) into the box at the top of the browser window. The Installation Wizard is displayed on screen and will guide you through the configuration described in the sections below.
4. Remember to change the IP address and subnet mask of you Management Station back to their original values when you have finished configuring the Firewall using the Installation Wizard.

Configuring Basic Settings

When the Installation Wizard first starts it displays a welcome screen shown in Figure 7 below.

Figure 7 Installation Wizard Startup Screen



Firewall Installation Wizard - Microsoft Internet Explorer

Welcome to the SuperStack 3 Firewall Installation Wizard

This Wizard will help you quickly configure the Firewall to secure your Internet connection. Once completed, you can use the Firewall Web interface for additional configuration options. Please see the User Guide for more details.

To bypass this Wizard, click "Cancel".

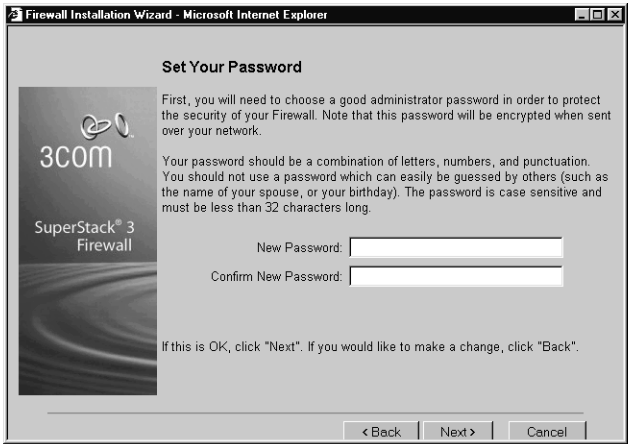
Click the *Next* button to start configuring your Firewall using the Installation Wizard. The *Set Your Password* screen will be displayed as shown in Figure 8 below.

If you want to configure your Firewall manually, click the Cancel button. You will then be returned to the Web interface. See "Configuring the Firewall" starting on page 49 to configure the Firewall using the Web interface.

Setting the Password

Choose an administration password end enter it in the *New Password* and *Confirm New Password* fields. This will be use in conjunction with the **`admin`** *User Name* when logging on to the Firewall in the future.

Figure 8 Set Password Screen



Firewall Installation Wizard - Microsoft Internet Explorer

Set Your Password

First, you will need to choose a good administrator password in order to protect the security of your Firewall. Note that this password will be encrypted when sent over your network.

Your password should be a combination of letters, numbers, and punctuation. You should not use a password which can easily be guessed by others (such as the name of your spouse, or your birthday). The password is case sensitive and must be less than 32 characters long.

New Password:

Confirm New Password:

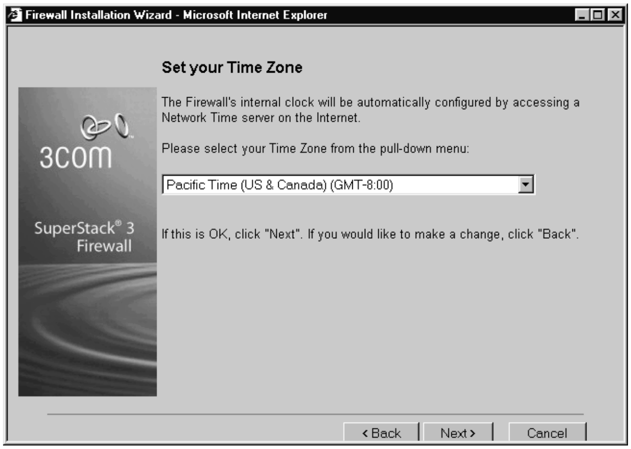
If this is OK, click "Next". If you would like to make a change, click "Back".

Click the *Next* button to continue.

Setting the Time Zone

Select the *Time Zone* appropriate to your location and click the *Next* button to continue. The Time Zone you choose will affect the time recorded in the logs.

Figure 9 Set Time Zone screen



Firewall Installation Wizard - Microsoft Internet Explorer

Set your Time Zone

The Firewall's internal clock will be automatically configured by accessing a Network Time server on the Internet.

Please select your Time Zone from the pull-down menu:

Pacific Time (US & Canada) (GMT-8:00)

If this is OK, click "Next". If you would like to make a change, click "Back".

This completes the Basic setup of the Firewall.

The Firewall will now attempt to configure some of its network settings automatically. If it is unable to detect the settings automatically the

Installation Wizard will prompt you for the required settings.

Configuring WAN Settings

The Installation Wizard detects if the Firewall has been automatically allocated an address for its WAN port.

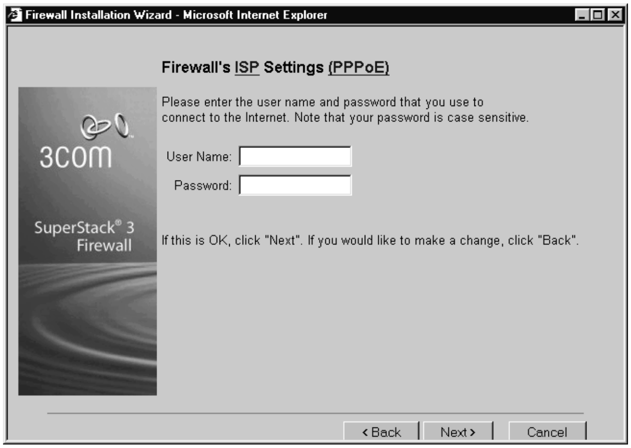
- If the Firewall has been allocated an IP address then it will attempt to configure itself automatically. See "Automatic WAN Settings" below.
- If the Firewall has not been allocated an IP address then it will prompt you for the settings it requires. See "Manual WAN Settings" on page 40.

Automatic WAN Settings

The Installation Wizard checks for the presence of a DHCP Server or a PPPoE server on the WAN port. Depending on the server found the Firewall configures itself appropriately as described below:

- *DHCP Server* — The Firewall requests an IP address form the DHCP server on the WAN Port and uses the IP address, subnet mask and any DNS information supplied
- *PPPoE Server* — The Installation Wizard prompts you to enter the User Name and Password supplied by your ISP. See Figure 10 below.

Figure 10 Configuring the Firewall's PPPoE settings



Firewall's ISP Settings (PPPoE)

Please enter the user name and password that you use to connect to the Internet. Note that your password is case sensitive.

User Name:

Password:

If this is OK, click "Next". If you would like to make a change, click "Back".

If the WAN Setup has completed successfully, go to "Configuring LAN Settings" on page 44.

Manual WAN Settings

If the Installation Wizard is unable to detect an automatic address server on the WAN Port or if the WAN port is not connected it will display a dialog box informing you of this and offer the choice of:

- Connecting your Firewall (if not already connected) and restarting the Installation Wizard.
- Configuring your Firewall manually.

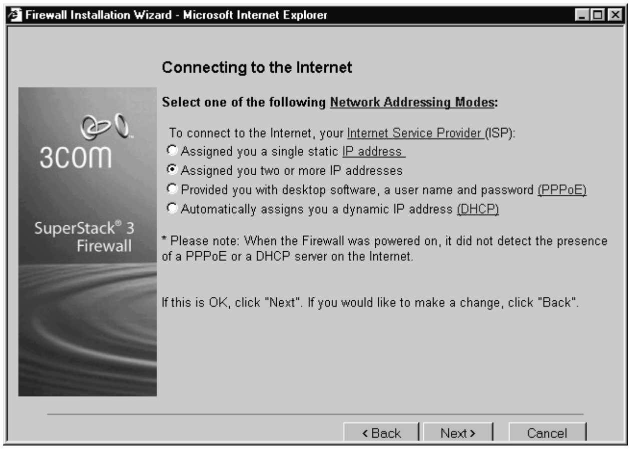
If you want to try to configure your Firewall again using the Installation Wizard's automatic detection then:

1. Disconnect the power cord from the Firewall.
2. Wait at least 5 seconds.
3. Reconnect the power cord.
4. Point your browser at the Firewall.
5. Follow the instructions supplied by the Installation Wizard.

If you want to configure the WAN settings of the Firewall manually then click the *Next* button to continue.

The Installation Wizard will display its *Connecting to the Internet* screen, shown in Figure 11 below. This allows you to specify the addressing mode you are using on your WAN port.

Figure 11 Specifying the connection on the WAN port



Connecting to the Internet

Select one of the following Network Addressing Modes:

To connect to the Internet, your Internet Service Provider (ISP):

○ Assigned you a single static IP address
● Assigned you two or more IP addresses
○ Provided you with desktop software, a user name and password (PPPoE)
○ Automatically assigns you a dynamic IP address (DHCP)

* Please note: When the Firewall was powered on, it did not detect the presence of a PPPoE or a DHCP server on the Internet.

If this is OK, click "Next". If you would like to make a change, click "Back".

The options are as follows:

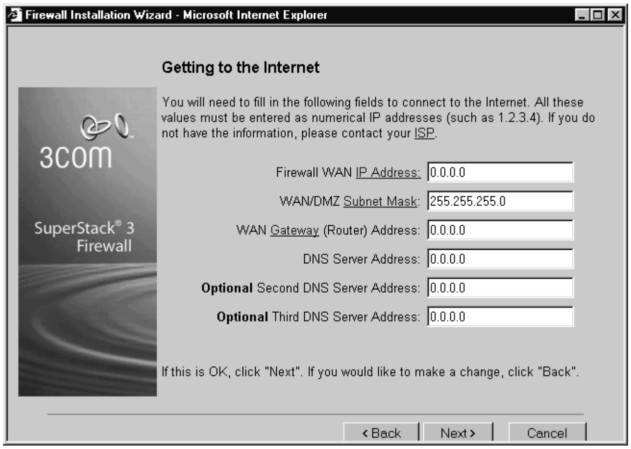
- Using a Single Static IP Address — This address must be taken by the Firewall's WAN port to allow devices connected to the LAN port to communicate with devices connected to the WAN port. Network Address Translation (NAT) will be enabled.
- Using Multiple Static IP Addresses — One address will be taken by Firewall's WAN port. NAT can be disabled sharing the addresses between the DMZ port and the LAN port or enabled leaving all the public addresses for the DMZ port. This option will be offered later in the *Installation Wizard*.
- Using an IP Address provided by a PPPoE Server — One IP address is provided by the PPPoE server. This is taken by the WAN port. Network Address Translation (NAT) will be enabled.
- Using a Static IP address provided by a DHCP Server — One IP address is provided by the DHCP server. This is taken by the WAN port. Network Address Translation (NAT) will be enabled.

The settings for each of these options are detailed in the following sections.

Using a Single Static IP Address

Select the *Assigned you a single static IP address option* and click the *Next* button. The *Getting to the Internet screen* will be displayed as shown in Figure 12 below.

Figure 12 Configuring the Firewall



Getting to the Internet

You will need to fill in the following fields to connect to the Internet. All these values must be entered as numerical IP addresses (such as 1.2.3.4). If you do not have the information, please contact your ISP.

Firewall WAN IP Address: 0.0.0.0
WAN/DMZ Subnet Mask: 255.255.255.0
WAN Gateway (Router) Address: 0.0.0.0
DNS Server Address: 0.0.0.0
Optional Second DNS Server Address: 0.0.0.0
Optional Third DNS Server Address: 0.0.0.0

If this is OK, click "Next". If you would like to make a change, click "Back".

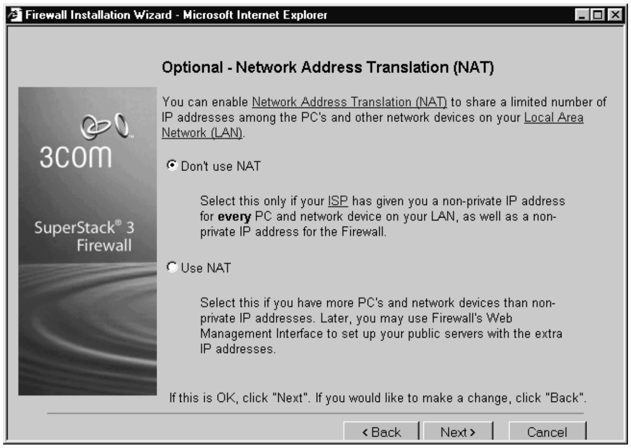
To configure the WAN networking of your Firewall enter the following

1. In the *Firewall WAN IP Address* field enter the single address which has been allocated to your Firewall. Enter the subnet mask for the above IP address in the *WAN/DMZ Subnet Mask* field.
2. In the *WAN Gateway (Router) Address* field enter the address of your internet access device. This may be a router, LAN modem or other device and must be in the same subnet as the WAN IP address of the Firewall.
3. Enter any DNS servers external to your network in the order that you want them to be accessed. The second server will only be accessed if the first is unavailable or is unable to answer your query.
4. Click the *Next* button to proceed to the final part of the configuration. See "Configuring LAN Settings" on page 44.

Using Multiple Static IP Addresses

Select the *Assigned you two or more IP addresses* option and click the *Next* button. The *Network Address Translation* screen will be displayed as shown in Figure 13 below.

Figure 13 Choosing whether to activate NAT for multiple addresses



Optional - Network Address Translation (NAT)

You can enable Network Address Translation (NAT) to share a limited number of IP addresses among the PC's and other network devices on your Local Area Network (LAN).

● Don't use NAT

Select this only if your ISP has given you a non-private IP address for **every** PC and network device on your LAN, as well as a non-private IP address for the Firewall.

○ Use NAT

Select this if you have more PC's and network devices than non-private IP addresses. Later, you may use Firewall's Web Management Interface to set up your public servers with the extra IP addresses.

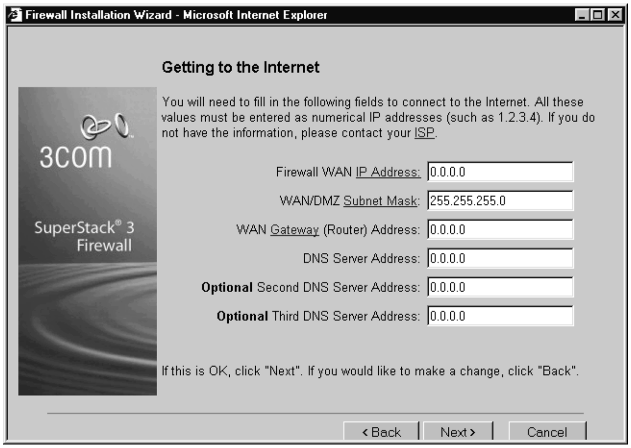
If this is OK, click "Next". If you would like to make a change, click "Back".

You are given a choice of:

- Don't use NAT — This will disable Network Address Translation, limiting you to the same number of IP devices as you have addresses.
- Use NAT — This will enable Network Address Translation allowing you to use as many IP devices as you wish on the LAN port. The remaining public IP addresses can be allocated to devices on the DMZ port.

Click the *Next* button to proceed to the *Getting to the Internet* screen shown in Figure 14 below.

Figure 14 Setting the Firewall WAN configuration



Getting to the Internet

You will need to fill in the following fields to connect to the Internet. All these values must be entered as numerical IP addresses (such as 1.2.3.4). If you do not have the information, please contact your ISP.

Firewall WAN IP Address: 0.0.0.0
WAN/DMZ Subnet Mask: 255.255.255.0
WAN Gateway (Router) Address: 0.0.0.0
DNS Server Address: 0.0.0.0
Optional Second DNS Server Address: 0.0.0.0
Optional Third DNS Server Address: 0.0.0.0

If this is OK, click "Next". If you would like to make a change, click "Back".

The *Getting to the Internet* screen contains the following fields:

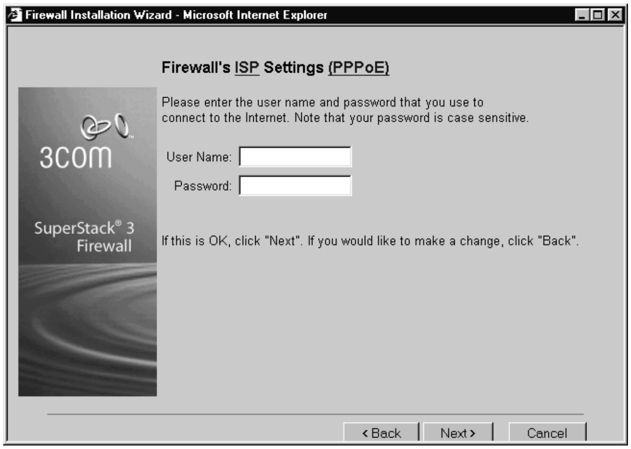
1. *Firewall WAN IP Address* — Choose one of the addresses allocated by your ISP as the address of the Firewall's WAN port. This is used for communication across the Firewall and to manage the Firewall remotely.
2. *WAN/DMZ Subnet Mask* — Enter the subnet mask that defines the IP address range supplied by your ISP.
3. *WAN Gateway (Router) Address* — Enter the IP address of your route or internet access device. This must be in the same address range as the *WAN IP Address*.
4. *DNS Server Address* — Enter the IP address of your ISP's DNS server in this field. This will be used to resolve machine names to IP addresses. If you have access to additional DNS Servers, enter them in the *Optional Second DNS Server Address* and *Optional Third DNS Server Address* fields. These will be accesses if the first stated DNS server does not respond or if it has no record of a device name.

Click the *Next* button to proceed to the final part of the configuration. See "Configuring LAN Settings" on page 44.

Using an IP Address provided by a PPPoE Server

Select the *Provided you with two or more IP addresses* option and click the *Next* button. The *Firewall's ISP Settings (PPPoE)* screen will be displayed as shown in Figure 15 below.

Figure 15 Configuring the Firewall's PPPoE settings



Firewall Installation Wizard - Microsoft Internet Explorer

Firewall's ISP Settings (PPPoE)

Please enter the user name and password that you use to connect to the Internet. Note that your password is case sensitive.

User Name:

Password:

If this is OK, click "Next". If you would like to make a change, click "Back".

Enter the *User Name* and *Password* as supplied by your ISP and click the Next button to proceed to the final part of the configuration. See "Configuring LAN Settings" on page 44.

Using a Static IP address provided by a DHCP Server

Select the *Automatically assigns you a dynamic IP address (DHCP)* option and click the *Next* button. If a DHCP server is detected the Firewall will obtain its IP address automatically and will enable NAT for all devices connected to the LAN port. Click the Next button again to confirm your choice and proceed to the final part of the configuration. See "Configuring LAN Settings" below.

Configuring LAN Settings

Once the WAN setting of the Firewall have been configured, the *Installation Wizard* configures the Firewall's LAN settings. Some of the following processes are optional and screens will only appear if they are relevant to the configuration of your Firewall.

Automatic LAN Settings

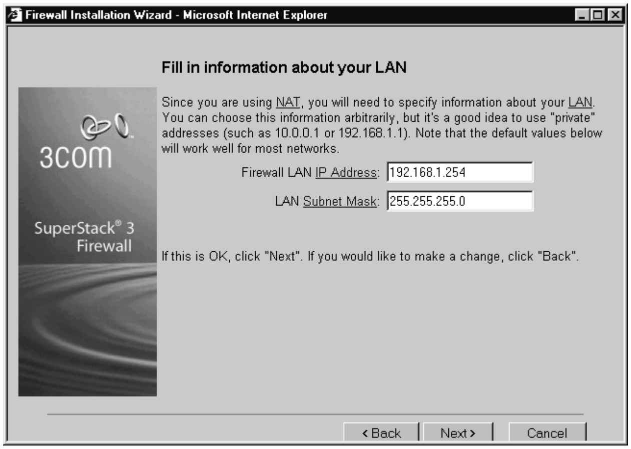
The *Installation Wizard* checks for the presence of a DHCP server on the LAN port.

- If there is no DHCP server found on the network connected to the LAN port then the Firewall's DHCP server is activated allowing automatic address configuration on your LAN.
- If there is a DHCP server found on the network connected to the LAN port then the Firewall deactivates its DHCP server. This prevents the Firewall giving out addresses that will conflict with those allocated by another server.

Entering information about your LAN

If you are using NAT the *Fill in information about your LAN* screen will appear as shown in Figure 16 below. If you are not using NAT this screen will not appear as these settings will be the same as the WAN settings.

Figure 16 Configuring LAN Settings



Fill in information about your LAN

Since you are using NAT, you will need to specify information about your LAN. You can choose this information arbitrarily, but it's a good idea to use "private" addresses (such as 10.0.0.1 or 192.168.1.1). Note that the default values below will work well for most networks.

Firewall LAN IP Address: 192.168.1.254

LAN Subnet Mask: 255.255.255.0

If this is OK, click "Next". If you would like to make a change, click "Back".

- Choose an IP address for the LAN port of your Firewall and enter it in the *Firewall LAN IP Address* field.
- Enter the Subnet mask for your LAN network in the *LAN Subnet Mask* field.

The default IP address of the Firewall is `192.168.1.254` *with a subnet mask of* `255.255.255.0`*. You may want to keep this setting as other 3Com products also have their default addresses in this range.*

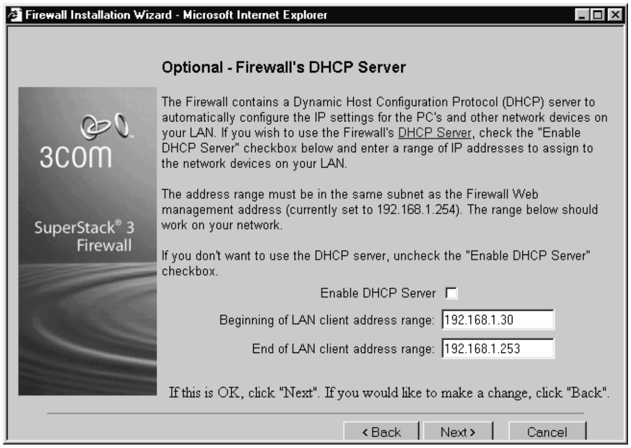
Click the *Next* button to continue.

Configuring the DHCP Server

If a DHCP server has been detected on your LAN network then the Firewall will disable its DHCP server and this screen will not display.

Otherwise the Firewall’s DHCP Server screen will be displayed as shown in Figure 17 below.

Figure 17 Configuring the Firewall’s DHCP Server



Optional - Firewall's DHCP Server

The Firewall contains a Dynamic Host Configuration Protocol (DHCP) server to automatically configure the IP settings for the PC's and other network devices on your LAN. If you wish to use the Firewall's DHCP Server, check the "Enable DHCP Server" checkbox below and enter a range of IP addresses to assign to the network devices on your LAN.

The address range must be in the same subnet as the Firewall Web management address (currently set to 192.168.1.254). The range below should work on your network.

If you don't want to use the DHCP server, uncheck the "Enable DHCP Server" checkbox.

Enable DHCP Server □

Beginning of LAN client address range: 192.168.1.30

End of LAN client address range: 192.168.1.253

If this is OK, click "Next". If you would like to make a change, click "Back".

If you want to use the Firewall as a DHCP server to automatically provide IP addresses for the computers on your LAN click the enable DHCP server box and set the range of addresses you want it to allocate.

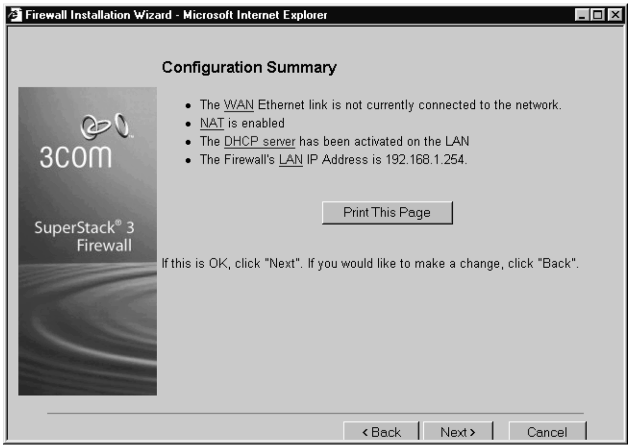
The addresses you set must be contained entirely within your LAN subnet and must be currently unused.

Click the *Next* button to continue. The Firewall will now review its settings. See “Confirming Firewall Settings” below for details.

Confirming Firewall Settings

The Firewall prompts you to confirm the settings it has established through automatic configuration as well as those entered manually. You will be presented with a screen similar to Figure 18 below showing you settings with which the Firewall has been configured.

Figure 18 Firewall Configuration Summary



Configuration Summary

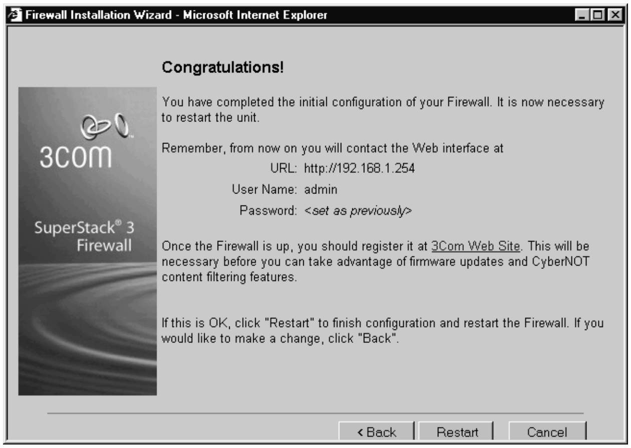
- The WAN Ethernet link is not currently connected to the network.
- NAT is enabled
- The DHCP server has been activated on the LAN
- The Firewall's LAN IP Address is 192.168.1.254.

If this is OK, click "Next". If you would like to make a change, click "Back".

- If you want to keep a hard copy of this page click the *Print This Page* button.
- To accept the settings click the *Next* button.
- To change the configuration of the Firewall click the *Back* button.
- If you want to configure the Firewall manually:
  - Click the *Cancel* button to lose the changes made by the Installation Wizard or
  - Click the *Next* Button, continue to the end of the Installation Wizard and make the changes once the Firewall has reset

If you click the *Next* button the following screen will display.

Figure 19 Congratulations Page



Congratulations!

You have completed the initial configuration of your Firewall. It is now necessary to restart the unit.

Remember, from now on you will contact the Web interface at

URL:	http://192.168.1.254
User Name:	admin
Password:	*<set as previously>*

Once the Firewall is up, you should register it at 3Com Web Site. This will be necessary before you can take advantage of firmware updates and CyberNOT content filtering features.

If this is OK, click "Restart" to finish configuration and restart the Firewall. If you would like to make a change, click "Back".

Click the *Restart* button to complete the configuration of the Firewall using the *Installation Wizard*.

The Firewall will take under a minute to restart during which time the Power/Self test LED will flash. When the Power/Self test LED stops flashing the Firewall is ready for use.

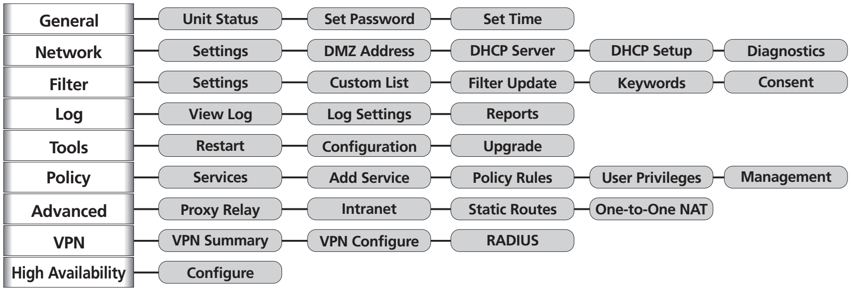
II CONFIGURING THE FIREWALL

4 BASIC SETTINGS OF THE FIREWALL

Chapters 4 to 10 describe in detail, each of the management operations available from the Firewall's web interface. You can access these operations using a Web browser.

Refer to Figure 20 below for menu structure details of the Web interface of the Firewall.

Figure 20 Tree Diagram of the menu structure



The descriptions of these menu options are split into chapters as follows:

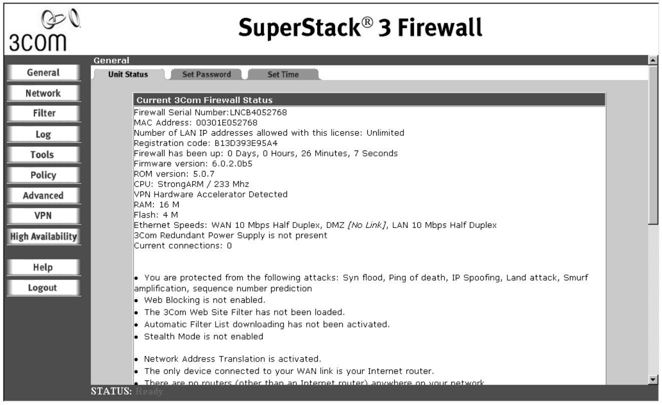
- Chapter 4 — This chapter describes the functions available in the *General* and *Network* menus of the Web interface. These functions are used to configure the Firewall for your network and location and are most frequently accessed when setting up or moving the Firewall or reconfiguring it for another role.
- Chapter 5 — "Setting up Web Filtering" describes the functions available in the *Filter* menu of the Web interface. These functions allow you to control the access your users have to information on the Web.
- Chapter 6 — "Using the Firewall Diagnostic Tools" describes the functions available in the *Log* and *Tools* menus of the Web interface. These functions allow you to monitor and manage your Firewall.

- Chapter 7 — "Setting a Policy" describes the functions available in the *Policy* menu of the Web interface. These functions enable you to control the traffic across your Firewall.
- Chapter 8 — "Advanced Settings" describes the functions available in the *Advanced* menu of the Web interface. These functions enable you to configure your Firewall for different topologies of network and to provide some of the functionality of a router within your network.
- Chapter 9 — "Configuring Virtual Private Network Services" describes the functions available in the *VPN* menu of the Web interface. These functions enable you encrypt and authenticate external access to your Firewall.
- Chapter 10 — "Configuring High Availability" describes the functions available in the *High Availability* menu of the Web interface. These functions allow you to set up a second SuperStack 3 Firewall as a live backup should your Firewall fail.

Examining the Unit Status

To display the Firewall Unit Status, click on the *General* button and click on the tab labelled *Unit Status*. A window similar to the following displays.

Figure 21 Unit Status Window



Current 3Com Firewall Status

```
Firewall Serial Number:LNCB4052768
MAC Address: 00301E052768
Number of LAN IP addresses allowed with this license: Unlimited
Registration code: B13D393E95A4
Firewall has been up: 0 Days, 0 Hours, 26 Minutes, 7 Seconds
Firmware version: 6.0.2.0b5
ROM version: 5.0.7
CPU: StrongARM / 233 Mhz
VPN Hardware Accelerator Detected
RAM: 16 M
Flash: 4 M
Ethernet Speeds: WAN 10 Mbps Half Duplex, DMZ [No Link], LAN 10 Mbps Half Duplex
3Com Redundant Power Supply is not present
Current connections: 0


• You are protected from the following attacks: Syn flood, Ping of death, IP Spoofing, Land attack, Smurf
amplification, sequence number prediction
• Web Blocking is not enabled.
• The 3Com Web Site Filter has not been loaded.
• Automatic Filter List downloading has not been activated.
• Stealth Mode is not enabled

• Network Address Translation is activated.
• The only device connected to your WAN link is your Internet router.
• There are no routers (other than an Internet router) anywhere on your network
```

This window shows the following information for your Firewall:

- Firewall Serial Number
- MAC Address
- Registration Code (once registered)

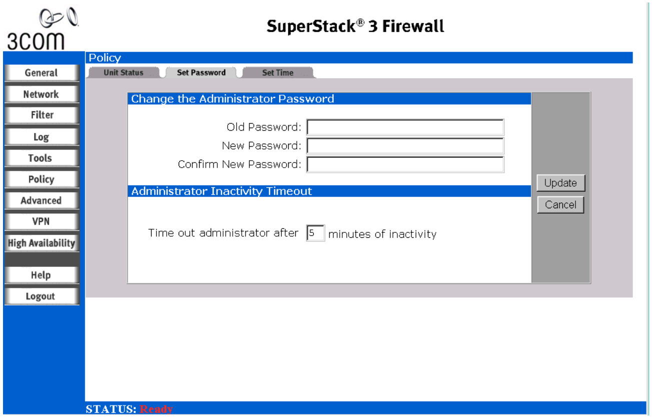
- ROM Version
- Firmware Version
- Device Up-time in days, hours, minutes, and seconds

Problems appear in red text. For example, if the Internet router was not contacted, or the default password was not changed, this would be listed. Items listed in red require immediate, corrective action. General operation status messages, such as enabled hacker attack protection, filter list status, and log settings are listed in black text.

Setting the Administrator Password

From the *General* screen, select *Set Passwor*d. A window similar to that in Figure 22 displays. If you are setting the password for the first time, the default password is “password”. Change the administrator password to keep the Firewall secure.

Figure 22 Set Password Screen



Change the Administrator Password

Old Password:

New Password:

Confirm New Password:

Administrator Inactivity Timeout

Time out administrator after 5 minutes of inactivity

STATUS: Ready

1. In the *Old Password* box, type the old password.
2. In the *New Password* and *Confirm New Password* boxes type the new password
3. Click *Update* to save the new password.

The password cannot be recovered if it is lost or forgotten.

***CAUTION:** If the password is lost, you must reset the Firewall. See “Resetting the Firewall” on page 162.*

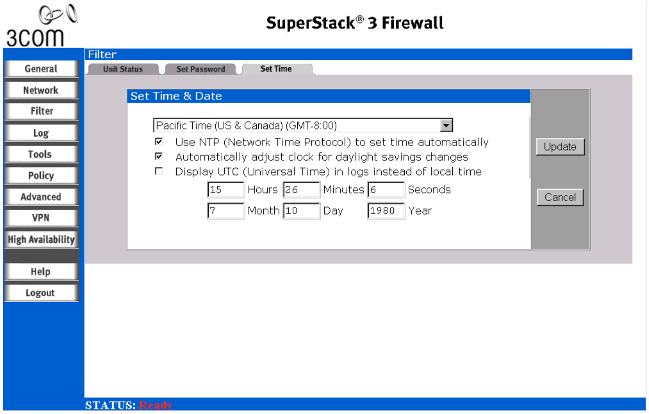
Setting the Inactivity Timeout

The Administrator Inactivity Timeout Setting allows you to extend or reduce the period of time before the administrator is automatically logged out of the Web interface. The Firewall is pre-configured to logout the administrator after 5 minutes of inactivity.

Setting the Time

From the *General* screen, select *Set Time*. A window similar to that in Figure 23 displays.

Figure 23 Set Time Window



Pacific Time (US & Canada) (GMT-8:00)

☑ Use NTP (Network Time Protocol) to set time automatically

☑ Automatically adjust clock for daylight savings changes

□ Display UTC (Universal Time) in logs instead of local time

15 Hours 26 Minutes 6 Seconds

7 Month 10 Day 1980 Year

STATUS: Ready

Time Zone

Select your time zone from the drop-down list box at the top of the screen. If you cannot find your time zone in the list, you should set this to the one with the same offset from GMT as is used at your location.

Use NTP (Network Time Protocol) to set time automatically

Check this box to allow the Firewall to synchronize its time using an Network Time Protocol (NTP) server every hour. For example, if you started the Firewall at 2:30, the clock will synchronize every hour at the half hour—3:30, 4:30 etc.

To set the time automatically you need a connection to the Internet. 3Com recommends that initially you set the time manually even if you have selected this option.
See Manual Time Set *below to set the time manually.*

Automatically adjust clock for daylight savings changes

Check this box to enable the Firewall to adjust to Daylight Savings Time automatically depending on the time zone you have chosen. This features works with NTP on or off.

Display UTC (Universal Time) in logs instead of local time

Check this box to set the time on the Firewall to Universal Time Co-ordinated (UTC) time. UTC is the standard time common to all places in the world. It is also commonly referred to as Greenwich Mean Time or World Time. Many ISPs require firewall logs to be recorded in UTC as tracking hackers can be very difficult if reports of times are not consistent.

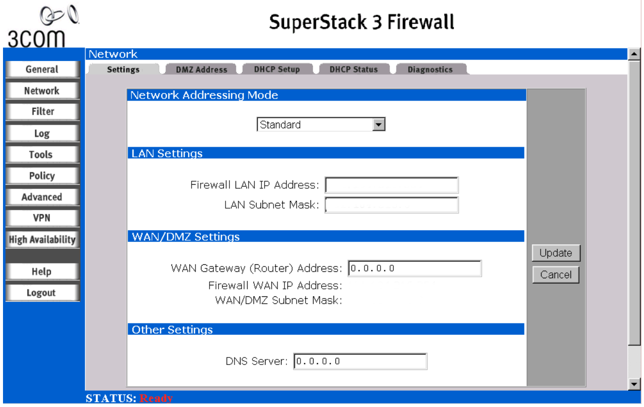
Manual Time Set

To set the time manually enter the date and time in the boxes at the bottom of the screen. Set the time in 24-hour clock, and use four digits to specify the year (for example, 2001).

Changing the Basic Network Settings

Click the *Settings* Tab from the *Network* Menu to display the *Network Settings* window (see Figure 24 below).

Figure 24 Network Settings, Standard Window



Network Addressing Mode

Standard

LAN Settings

Firewall LAN IP Address:

LAN Subnet Mask:

WAN/DMZ Settings

WAN Gateway (Router) Address: 0.0.0.0

Firewall WAN IP Address:

WAN/DMZ Subnet Mask:

Other Settings

DNS Server: 0.0.0.0

STATUS: Ready

Setting the Network Addressing Mode

The *Network Addressing Mode* drop-down list contains four modes:

Standard

Choose *Standard* if you have IP addresses allocated by your ISP for each machine that requires access to the Internet. When you select *Standard*, Network Address Translation (NAT) is disabled. All nodes on the LAN must use a valid public IP address.

NAT Enabled

Choose *NAT Enabled* if you want to use a single IP address for accessing the Internet, or if you do not have an IP address allocated by your ISP for each machine that requires access to the Internet. NAT provides anonymity to machines on the LAN by connecting the entire network to the Internet using a single IP address. This is useful for two purposes:

- Additional security is provided because all the addresses on the LAN are invisible to the outside world.
- In cases where a network uses invalid IP addresses or if addresses are in short supply, NAT can be used to connect the LAN to the Internet without changing the IP addresses of computers and other devices on the LAN.

Remote authenticated access is not possible with NAT enabled.

When using IP addresses on a LAN which have not been assigned by an Internet Service Provider, it is a good idea to use addresses from a special address range allocated for this purpose. The following IP address ranges can be used for private IP networks and do not get routed on the Internet:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

Select *NAT Enabled* from the *Network Addressing Mode* drop-down list if the network uses private IP addresses or if addresses are in short supply.

NAT with DHCP Client

Choose *NAT with DHCP Client* if you obtain the Firewall WAN IP address from a remote DHCP server.

NAT with PPPoE Client

Choose *NAT with PPPoE Client* if your Internet connection for the Firewall WAN IP Address is to be obtained from a remote PPPoE server.

Specifying the LAN Settings

For the LAN settings, specify:

Firewall LAN IP Address.

This is the IP address that is given to the Internet Firewall and used to access it for configuration and monitoring. Choose a unique IP address from the LAN address range.

LAN Subnet Mask

This value is used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address.

For example, consider the IP address `192.168.228.17.` Assuming a Class C subnet mask of `255.255.255.0` is used, the first three numbers (`192.168.228.`) represent the Class C network address, and the last number (`17`) identifies a particular host on this network.

The following setting will also be available if PPPoE is selected:

Connect/Disconnect

Pressing the *Connect* button in the Network Addressing Mode Section will initiate a PPPoE session. If all fields have been entered correctly, the Firewall will connect to the Internet. You can terminate a PPPoE session by pressing the *Disconnect* button.

Specifying the WAN/DMZ Settings

For the WAN/DMZ settings, specify:

WAN Gateway (router) Address

The WAN gateway address, also called the default gateway, is the address of the router that attaches the LAN to the Internet.

Firewall WAN IP Address

This value is automatically set to the LAN IP Address for the Firewall unless PPPoE is selected. For PPPoE enter the value specified by your ISP.

WAN/DMZ Subnet Mask

This value is automatically set to the LAN Subnet Mask for the Firewall unless PPPoE is selected. For PPPoE enter the value specified by your ISP.

If PPPoE is selected, you also have to set the following:

User Name

Enter the *User Name* for your PPPoE account in this section. This is information given to you by your service provider upon initial installation of your broadband service.

Password

Enter the *Password* for your PPPoE account in this section. This is information given to you by your service provider upon initial installation of your broadband service.

Gateway (Router) Address:

This address will be provided automatically by your service provider.

For more information about PPPoE refer to “Frequently Asked Questions about PPPoE” in Chapter 12.

Specifying the DNS Settings

In the *Other Settings* section, specify the *DNS Serve*rs. Up to three DNS servers can be specified, although not all have to be used. The Firewall uses these servers to look up the addresses of machines used to download the Web Site Filter and for the built-in *DNS Lookup* tool.

Type the required values and click *Update* to save the changes. It is necessary to restart the Firewall for these changes to take effect.

Specifying DMZ Addresses

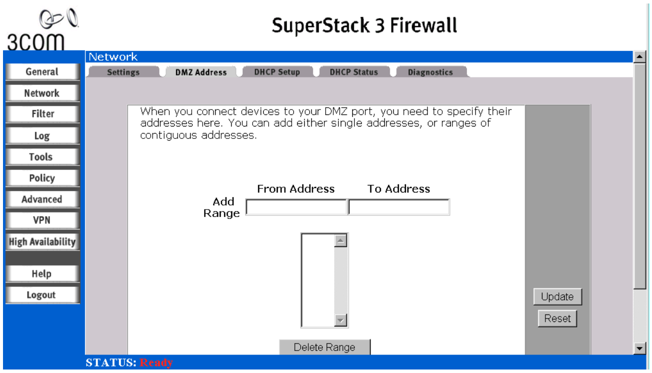
The Firewall provides security by preventing Internet users from accessing machines inside the LAN. This security, however, also prevents users from reaching servers intended for public access, such as a Web or e-mail server, which are crucial for effective Internet use.

In order to allow such services, the Firewall comes with a special *Demilitarized Zone* (DMZ) port which you use for setting up public servers. The DMZ is located between the local network and the Internet. Servers on the DMZ are publicly accessible, but they are protected from attacks such as SYN Flooding and Ping of Death. Use of the DMZ port is optional and you do not have to connect it.

3Com recommends that you use the DMZ port as an alternative to Public LAN Servers or to putting these servers on the WAN port where they are not protected and not accessible by users on the LAN unless intranet features are enabled.

Click *Network*, and then select the *DMZ Addresses* tab. A window similar to that in Figure 25 displays.

Figure 25 DMZ Address Window



When you connect devices to your DMZ port, you need to specify their addresses here. You can add either single addresses, or ranges of contiguous addresses.

Type the addresses for the DMZ individually or as a range. Type an individual address in the *From Address* box. To enter a range of addresses, such as the IP addresses from `199.168.23.50` to `199.168.23.100`, type the starting address in the *From Address* box and the ending address in the *To Address* box. You can specify up to 64 address ranges.

Each of the servers on the DMZ needs a public IP address. Obtain these IP addresses from your ISP. Usually, the ISP can also supply information on setting up public Internet servers.

Click the *Update* button to save your changes.

To delete an address or range, select it in the *Address Range* list and click *Delete*.

Network Address Translation (NAT) does not apply to servers on the DMZ. Servers on the DMZ Port must therefore have addresses in the same range as the WAN Port.

Setting up the DHCP Server

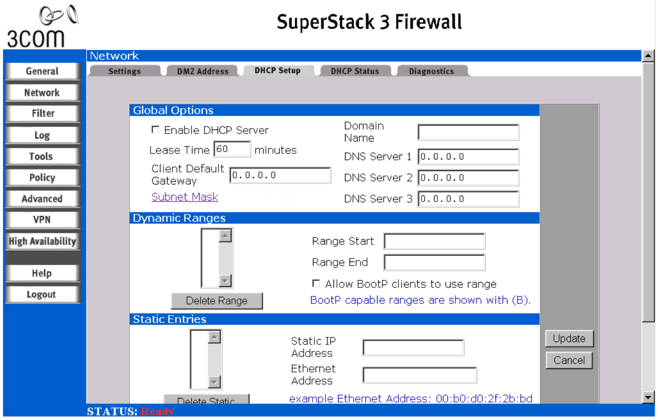
Dynamic Host Configuration Protocol (DHCP), is a means for computers on a network to obtain their IP settings from a centralized server.

DHCP offers complete centralized management of IP client configurations, including IP addresses, gateway address, and DNS address.

The Firewall can allocate up to 255 static or dynamic IP addresses. 3Com recommends you use a dedicated DHCP server if more addresses are required.

To set up the DHCP server on the Firewall click *Network*, and then select the *DHCP Server* tab. A window similar to that in Figure 26 displays.

Figure 26 DHCP Setup Window



Global Options

□ Enable DHCP Server

Lease Time 60 minutes

Client Default Gateway 0.0.0.0

Subnet Mask

Domain Name

DNS Server 1 0.0.0.0

DNS Server 2 0.0.0.0

DNS Server 3 0.0.0.0

Dynamic Ranges

Range Start

Range End

□ Allow BootP clients to use range

BootP capable ranges are shown with (B).

Static Entries

Static IP Address

Ethernet Address

example Ethernet Address: 00:b0:d0:2f:2b:bd

STATUS: Ready

Global Options

Enable DHCP Server

Click this check box to enable or disable the DHCP server. This is disabled by default. Leave the DHCP server disabled if there already is a DHCP server on the LAN or if manual addressing is used on the LAN computers.

Lease Time

This is the amount of time that the IP address is leased, or given to the client machine before the DHCP server attempts to renew that address. If the client still requires the use of the IP address, the DHCP Server grants the client the use of that IP address for the same amount of time. If the client no longer requires the IP address, the address is freed and returned to the pool of available addresses to be used again. The default value is 60 minutes.

Client Default Gateway

Enter the IP address of the WAN router used by LAN clients to access the Internet. If NAT is being used this will be the LAN IP address of the Firewall.

Subnet Mask

Enter the Subnet mask for your network. This value will be given out by the DHCP server and will be used by client devices to determine the extent of your network.

Domain Name

Type the registered domain name for the network in the *Domain Name* box, for example: `3com.com.` If you do not have a Domain Name leave this blank.

DNS Servers

A DNS Server translates human readable host names into the numeric IP addresses used by computers to route information to the correct machine. You can use multiple DNS servers to improve performance and reliability. To specify these manually select the *Specify Manually* radio box and type the IP address of the DNS Server(s) in these boxes.

Alternatively, if you are using NAT with DHCP client you can select the *Set DNS Servers by Internet Firewalls DHCP Client* to have these fields set automatically.

Dynamic Ranges

When a client makes a request for an IP address, the Firewall's DHCP server leases an address from the Dynamic Ranges.

Prior to offering an address from the Dynamic Range to a requesting client, the Firewall first verifies that the address is not already in use by another machine on the LAN.

To create a range of dynamic IP addresses to be assigned to requesting clients, type the starting number in the *Range Start* box, the ending address in the *Range End* box and then click *Updat*e.

Allow BootP clients to use range

Click this check box to have Dynamic BootP clients configured when they boot. Dynamic BootP clients are BootP clients that do not have an IP address assigned to their MAC address. They are similar to DHCP clients with the exception that leases are not supported.

Delete Range

To remove a range of addresses from the dynamic pool, select it from the scrolling list of dynamic ranges, and click *Delete Range*.

Static Entries

Static addresses are used by client machines that support BootP or those which require a fixed IP address. For example, client machines running Web or FTP servers require static addresses.

To create a static IP address to be assigned to a requesting client, type an IP address and the Ethernet (MAC) address of the client machine in the appropriate boxes and click *Update*.

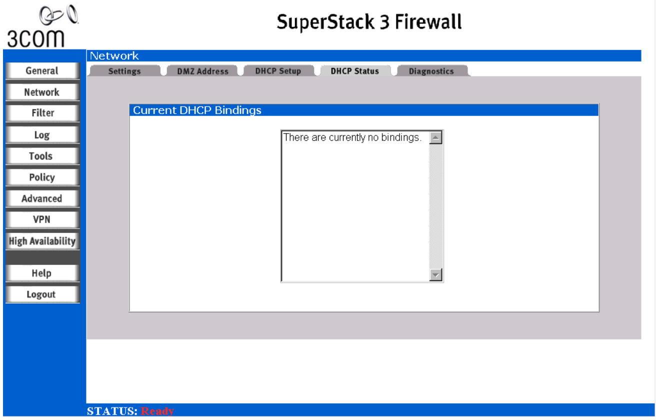
Delete Static

To remove a static address, select it from the scrolling list of static addresses and click *Delete Static*.

Viewing the DHCP Server Status

Click *Network* and then select the *DHCP Server Status* tab. A window similar to that in Figure 27 displays.

Figure 27 DHCP Status Window



There are currently no bindings.

STATUS: Ready

The scrolling window shows the details on the current bindings:

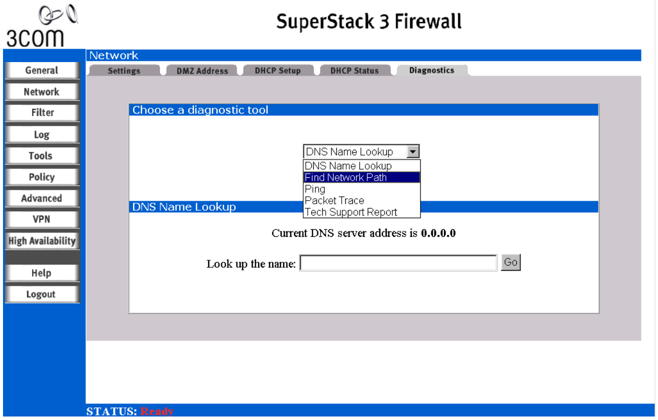
- IP and MAC address of the bindings
- Type of binding (Dynamic, Dynamic BootP, or Static BootP).

To delete a binding, which frees the IP address in the DHCP server, select the binding from the list and then click *Delete.*

Using the Network Diagnostic Tools

The Firewall has several tools built in which can help you solve network problems. Click *Network,* and then select the *Diagnostics* tab.

Figure 28 Diagnostics Window with Pull-down Menu



Current DNS server address is **0.0.0.0**

Look up the name:

STATUS: Ready

Choosing a Diagnostic Tool

The drop-down box provides five diagnostic tools:

DNS Name Lookup

Domain Name Service (DNS) is an internet service which allows users to enter an easily remembered host name, such as `www.3Com.com`, instead of numerical IP addresses to access Internet resources. The Firewall has a *DNS Lookup* tool that returns the numerical IP address of a host name.

1 Select *DNS Name Lookup* from the *Choose a diagnostic tool* menu.

2 Type the host name to lookup in the *Look up the name* box and click *Go*. The Firewall then queries the DNS server and displays the result at the bottom of the screen.

The IP address of at least one DNS Server must be present on the Network Settings *tab for the* DNS Name Lookup *feature to function.*

Find Network Path

Use the *Find Network Path* tool to show on which port, LAN, WAN or DMZ where appropriate, an IP host is located. This is helpful to determine if the Firewall is properly configured. For example, if the Firewall *thinks* that a machine known to be on the Internet is located on the LAN port, then there is a problem with the configuration of the network or intranet settings. *Find Network Path* also shows if the target node is behind a router, and the Ethernet address of the target node or router. *Find Network Path* also shows which router a node is using, which can help isolate router configuration problems.

1 Select *Find Network Path* from the *Choose a diagnostic tool* menu.

2 Type the IP address of the device and click *Go*. The test takes a few seconds to complete.

If the network path is incorrect, check the intranet, static route, and DMZ settings.

Find Network Path *requires an IP address. Use the Firewall's* DNS Name Lookup *tool to find the IP address of a host.*

Ping

The *Ping* tool bounces a packet off a machine on the Internet back to the sender. This test shows if the Firewall is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or other machine at the ISP's location. If this test is successful, try pinging devices outside the ISP. This shows if the problem lies with the ISP's connection.

1 Select *Ping* from the *Choose a diagnostic tool* menu.

2 Type the IP address of the device being pinged and click *Go*. The test takes a few seconds to complete.

Ping *requires an IP address. Use the Firewall's* DNS Name Lookup *tool to find the IP address of a host.*

Packet Trace

Use the *Packet Trace* tool to track the status of a data packet or communications stream as it moves from source to destination. This is a useful tool to determine if a packet or communications stream is being stopped at the Firewall, or is lost on the Internet.

Select *Packet Trace* from the *Choose a diagnostic tool* drop-down list.

Packet Trace *requires an IP address. Use the Firewall's* DNS Name Lookup *tool to find the IP address of a host.*

1 Enter the IP address of the remote host in the *Trace on IP address* box, and click *Start*.

2 Initiate an IP session with the remote host using an IP client, such as Web, FTP, or Telnet.

   Use the IP address in the *Trace on IP address* box, not a host name, such as `www.3Com.com.`

3 Click *Refresh* to display the packet trace information.

4 Click *Stop* to terminate the packet trace, and *Reset* to clear the results.

Technical Support Report

The *Tech Support Report* generates a detailed report of the Firewall's configuration and status, and saves it to the local hard disk. You can then e-mail this file to Technical Support to help assist with a problem.

1 Select *Tech Support Report* from the *Choose a diagnostic tool* menu.

2 Click *Save Report* to save the report as a text file to the local disk.

5 SETTING UP WEB FILTERING

This chapter describes the commands and options available in the *Filter* menu. The menu is broken up into five sections shown in the user interface as tabs.

To access a command click on *Filter* on the left hand side of the screen and then on the appropriate tab.

This following sections are covered in this chapter:

- Changing the Filter Settings
- Filtering Web Sites using a Custom List
- Updating the Web Filter
- Blocking Websites by using Keywords
- Filtering by User Consent

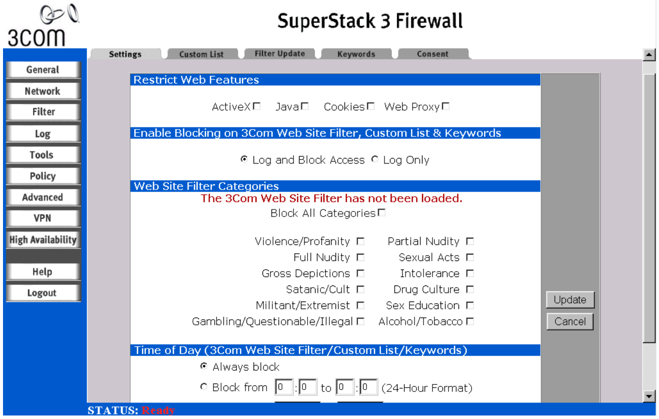
See Chapter 11 for background information about web filtering.

Changing the Filter Settings

Click *Filter*, and then select the *Settings* tab.

A window similar to that in Figure 29 displays.

Figure 29 Filter Settings Window



Restrict Web Features

ActiveX □ Java □ Cookies □ Web Proxy □

Enable Blocking on 3Com Web Site Filter, Custom List & Keywords

● Log and Block Access ○ Log Only

Web Site Filter Categories

The 3Com Web Site Filter has not been loaded.

Block All Categories □

Violence/Profanity □ Partial Nudity □
Full Nudity □ Sexual Acts □
Gross Depictions □ Intolerance □
Satanic/Cult □ Drug Culture □
Militant/Extremist □ Sex Education □
Gambling/Questionable/Illegal □ Alcohol/Tobacco □

Time of Day (3Com Web Site Filter/Custom List/Keywords)

● Always block
○ Block from 0 : 0 to 0 : 0 (24-Hour Format)

STATUS: Ready

Content Filtering only applies to nodes on the LAN Port.

Select the options in the *Settings* window, described below, to tailor the content filtering to meet the needs of your organization.

Restricting the Web Features Available

The following is a list of the web features that you can control using the Web Filter. To allow your network to access a category leave the checkbox unchecked. To deny your network access to a category check the checkbox corresponding to that category.

ActiveX

ActiveX is a programming language that is used to embed small programs in Web pages. It is generally considered an insecure protocol to allow into a network since it is possible for malicious programmers to write controls that can delete files, compromise security, or cause other damage.

Java

Java is also used to embed small programs, also called applets, in Web pages. It is generally considered safer than ActiveX since it has more thorough safety mechanisms. However, some administrators may choose to filter out Java since there have been instances of bugs in these safety mechanisms.

Cookies

Cookies are used by Web servers to track usage. Unfortunately, cookies can be programmed not only to identify the visitor to the site, but also to track that visitor's activities. Because they represent a potential loss of privacy, some administrators may choose to block cookies.

Web Proxy

When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server. This feature disables access to proxy servers located on the WAN. It has no effect on those located on the LAN.

Setting Blocking Options

The following is a list of the two alternative blocking options:

Log and Block Access

When selected, the Firewall logs and blocks access to all sites on the Web Site Filter, custom, and keyword lists.

Log Only

When selected, the Firewall logs and then allows access to all sites on the Web Site Filter, custom, and keyword lists. Use this function to monitor inappropriate usage without restricting access.

Specifying the Categories to Filter

The Web Site Filter can control access from the LAN to thousands of Web sites that might be deemed inappropriate for your organization. Twelve selectable Web site categories are provided so Internet access can be tailored to the needs of the organization. Check the boxes for those categories you wish to block. See “Introducing the Web Site Filter” on page 153 for a detailed explanation.

- Violence/Profanity
- Partial Nudity
- Full Nudity
- Sexual Acts
- Gross Depictions
- Intolerance
- Satanic/Cult

- Drugs/Drug Culture
- Militant/Extremist
- Sex Education
- Questionable/Illegal & Gambling
- Alcohol & Tobacco

Visit `http://www.cyberpatrol.com/cybernot` *to check the listing of a site or to submit a new site.*

Specifying When Filtering Applies

Use the *Time of Day* setting to define time periods during which Internet filtering is enabled. For example, in a school, it might be useful to enable Internet filtering during normal school hours to protect students, but to disable it after hours to give teachers complete access to the Internet. Similar policies could be enabled to allow employees complete access to the Internet after normal business hours.

Time of Day restrictions only apply to the Web Site Filter, Custom Sites, and Keywords. Consent and Restrict Web Features, such as ActiveX, Java, cookies and Web Proxy, are not affected.

Always Block

When selected, Internet Filtering is always active and Time of Day limitations are not enforced. This is enabled by default.

Block Between

When selected, Internet Filtering is only active during the time interval and days specified.

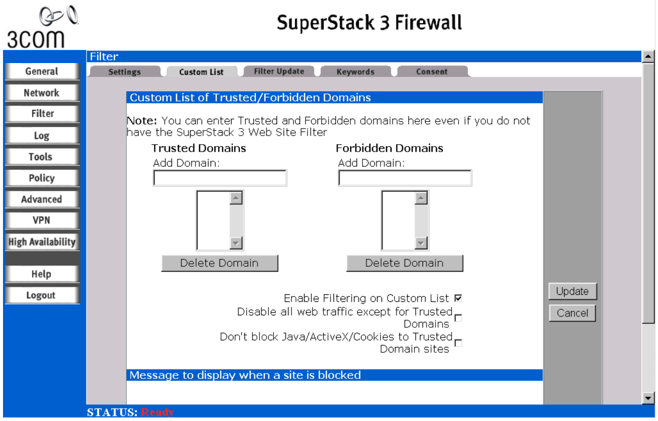
Enter the time period, in 24-hour format, and the start and end day of the week during which you want to enforce Internet Filtering.

Filtering Web Sites using a Custom List

This function allows you to block specific web sites, or restrict access to a list of approved web sites. This is in addition to the Web Site Filter. and overrides the more general Web Site Filter categories.

Click *Filter*, and then select the *Custom List* tab. A window similar to that in Figure 30 displays.

Figure 30 Custom List Window



Custom List of Trusted/Forbidden Domains

Note: You can enter Trusted and Forbidden domains here even if you do not have the SuperStack 3 Web Site Filter

Enable Filtering on Custom List ☑

Disable all web traffic except for Trusted Domains ☐

Don't block Java/ActiveX/Cookies to Trusted Domain sites ☐

Message to display when a site is blocked

STATUS: Ready

You can add or remove web sites from the Custom List. For example, if a local radio station runs a contest on its Web site that is disrupting normal classroom Internet use, a school’s Technology Coordinator can easily add that site to the *Forbidden Domains* list.

Setting up Trusted and Forbidden Domains

Trusted Domains — To allow access to a Web site which has been blocked by the Web Site Filter, type its host name, such as **`www.ok-site.com`**, into the *Trusted Domains* box. Do not use the complete URL of the site, that is, do not include **`http://`**. All subdomains are allowed. For example, adding **`3Com.com`** also allows **`www.3Com.com, my.support.3com.com, shop.3com.com`** and so forth. Up to 256 entries are supported in the *Trusted Domains* list. Click *Update* to send the update to the Firewall.

Forbidden Domains — To block a Web site which has not been blocked by the Web Site Filter, type its host name, such as **`www.bad-site.com`** into the *Forbidden Domains* box. Do not use the complete URL of the site, that is, do not include **`http://`**. All subdomains are blocked. For example, adding **`bad-site.com`** also blocks **`www.bad-site.com, my.support.bad-site.com, shop.bad-site.com`** and so forth. Click the *Update* button to save your changes.

To remove a site which was previously added, select its name in the list box, and click *Delete Domain* to send the update to the Firewall.

The following list describes the remaining options on the *Custom List* tab:

Enable Filtering on Custom List

Use this to enable or disable the custom filtering without re-entering all site names. You do not have to re-enter names when the Web Site Filter is updated each week, as the custom list does not expire.

Disable all Web traffic except for Trusted Domains

Click the *Disable Web traffic except for Trusted Domains* check box to allow Firewall Web access only to sites on the *Trusted Domains* list. With careful screening, this can block almost all objectionable material.

Don’t block Java/ActiveX/Cookies to Trusted Domains

Click this check box to make the Firewall allow Java, ActiveX and cookies from sites on the *Trusted Domains* list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or cookies from sites that are known and trusted.

Changing the Message to display when a site is blocked

When a user attempts to access a site that is blocked by the Web Site Filter, a message is displayed on their screen. The default message is:

```
Web Site Blocked by 3Com SuperStack 3 Firewall.
```

You can type any message, including embedded HTML, up to 255 characters long in this box.

For example, if you type the following:

```
Access to this site was denied because it appears to
violate this organization’s
<A HREF=http://www.your-domain.com/acceptable_use_policy.h
tm>Acceptable Use Policy</A>. Please contact the
<A HREF=”mailto:admin@your-domain.com”>Network
Administrator</A> if you feel this was in error.
```

The user will see the following displayed when they attempt to visit a blocked site:

```
Access to this site was denied because it appears to
violate this organization’s Acceptable Use Policy. Please
contact the Network Administrator if you feel this was in
error.
```

Where the underlined sections are links to your company’s acceptable use policy and to the network administrator’s email address.

Updating the Web Filter

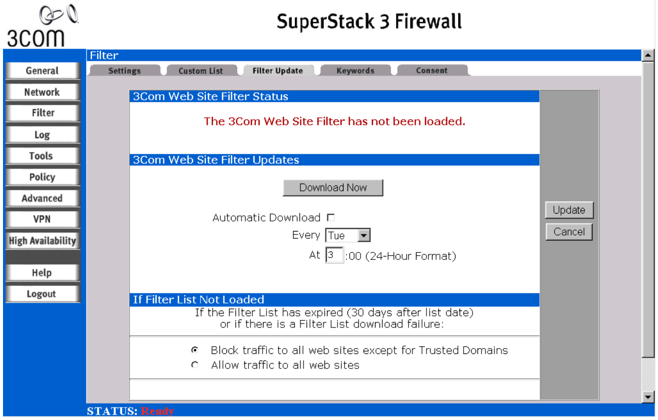
Since content on the Internet is constantly changing, make sure you update the Web Site Filter used by the Firewall on a regular basis. When you subscribe to the Web Site Filter, you can specify that it is updated automatically every week for one year.

It is important to note that host names, and not IP addresses, are used for all Internet filtering functions two reasons:

- Many blocked sites operate server pools, where many machines service a single host name, making it impractical and difficult to add and maintain the numerical addresses of every server in the pool.
- Many sites included in the Web Site Filter regularly change the IP address of the server to try to bypass the Web Site Filters. This makes maintaining a current list subscription critical for effective content filtering.

Click *Filter*, and then select the *Filter Update* tab at the top of the window. A window similar to that in Figure 31 displays.

Figure 31 Filter Update Window



3Com Web Site Filter Status

The 3Com Web Site Filter has not been loaded.

3Com Web Site Filter Updates

Automatic Download □

Every Tue

At 3 :00 (24-Hour Format)

If Filter List Not Loaded

If the Filter List has expired (30 days after list date)
or if there is a Filter List download failure:

● Block traffic to all web sites except for Trusted Domains
○ Allow traffic to all web sites

Checking the Web Filter Status

This section shows the status of the Web Site Filter and the date it was last downloaded. If the Web Site Filter has not been downloaded the Firewall displays a warning message in red text.

Downloading an Updated Filter List

Download Now

Click this button to download and update the Web Site Filter immediately. This process may take a couple of minutes, depending on Internet traffic conditions and requires a valid subscription to the Web Site Filter.

Automatic Download

Check this box to enable automatic, weekly updates to the Web Site Filter. Also, select the day of the week and the time of the day to download the new list. A valid Web Site Filter subscription is required.

Setting Actions if no Filter List is Loaded

There are two radio buttons that determine what happens if the Filter List expires or if a download of a Filter List fails:

Block traffic to all websites except for Trusted Domains

Select this option if only access to Trusted Domains should be available in the event of the Filter List expiring or a download failing. See "Setting up Trusted and Forbidden Domains" on page 71 for more information.

Allow traffic to all websites

Select this option to provide open access to the internet in the event of the Filter List expiring or a download failing.

Since it is necessary to restart the Firewall once the download is complete, which causes a momentary interruption of Internet access, it is a good idea to download new lists when LAN access to the Internet is at a minimum.

Click *Update* to save your changes.

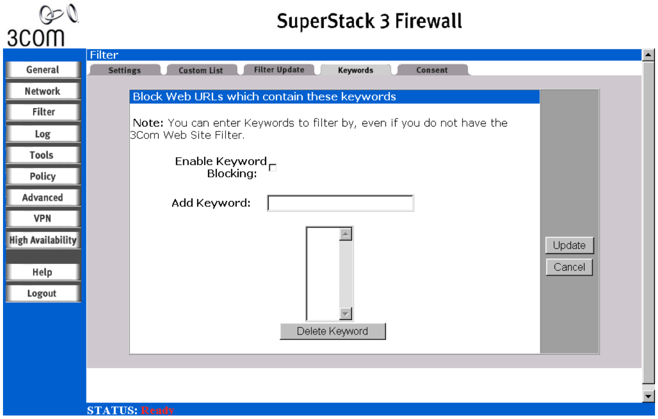
Once loaded, the creation date of the current active list is displayed at the top of the window.

Each download of the Web Site Filter expires 30 days after it is downloaded. The Filter List may also be erased if the Firewall fails to download a new list. If the Filter List expires or is erased, the Firewall may be configured to block all Web Sites except for Trusted Domains, or to allow access to all Web Sites.

Blocking Websites by using Keywords

Click *Filter* and then select the *Keywords* tab. A window similar to that in Figure 32 displays.

Figure 32 Keywords Window



Block Web URLs which contain these keywords

Note: You can enter Keywords to filter by, even if you do not have the 3Com Web Site Filter.

Enable Keyword Blocking: □

Add Keyword:

You can block Web URLs that contain specified keywords. This functions as a second line of defense against objectionable material. For example, if you specify the keyword ***xxx***, the following URL:

`http://www.new-site.com/xxx.html`

is blocked, even if it is not included in the Web Site Filter.

It is important to use caution when enabling this feature. For example, blocking the word breast *may stop access to sites on breast cancer as well as objectionable or pornographic sites.*

To enable this function check the *Enable Keyword Blocking* check box and click *Update*.

To add a keyword, in the *Add Keyword* box, type the keyword to block and click *Update*.

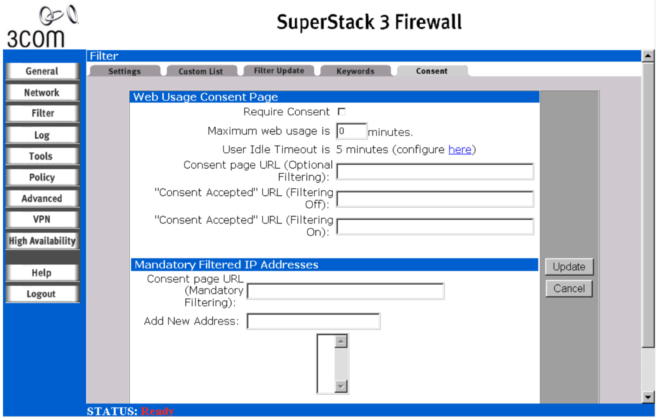
To remove a keyword, select it from the list and click *Delete Keyword*.

Filtering by User Consent

Use the *Consent* tab on the Filter menu to specify which computers are always filtered and which are filtered only when such protection is requested by the user. You can also configure *Consent* to require users to agree to the terms outlined in an organization’s *Acceptable Use Policy* before you allow them to browse the Web any further.

Click *Filter*, and then select the *Consent* tab. A window similar to that in Figure 33 displays.

Figure 33 Consent Window



Web Usage Consent Page

Require Consent □

Maximum web usage is 0 minutes.

User Idle Timeout is 5 minutes (configure here)

Consent page URL (Optional Filtering):

"Consent Accepted" URL (Filtering Off):

"Consent Accepted" URL (Filtering On):

Mandatory Filtered IP Addresses

Consent page URL (Mandatory Filtering):

Add New Address:

STATUS: Ready

Configuring User Consent Settings

Require Consent

Check this box to enable the consent features.

Maximum web usage is

In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. You can set up the Firewall to remind users when their time has expired by displaying the page defined in the *Consent page URL* box. Type the time limit, in minutes, in the *Maximum web usage is* box. Specify the default value of zero (0) to disable this feature.

User idle timeout

After a period of inactivity, the Firewall requires the user to agree to the terms outlined in the *Consent* tab before it allows any additional Web browsing. To configure the value, follow the link to the *User Privileges* window and type the desired value in the *Privileged User Idle Timeout* box.

Consent page URL (Optional Filtering)

When users begins an Internet session on a computer that is not always filtered, they are shown a consent page and given the option to access the Internet with or without filtering.

Create this page in HTML. It may contain the text from, or links to your company's *Acceptable Use Policy* (*AUP*).

You must include in this page links to two pages contained in the Firewall which, when selected, tell the Firewall if the user wishes to have filtering enabled or disabled. The link for unfiltered access must be:
`192.168.1.254/iAccept.html`

The link for filtered access must be:
`192.168.1.254/iAcceptFilter.html`

If you have changed the IP address or the Firewall use the IP Address of the Firewall instead of `192.168.1.254`.

Both the link for filtered access and the link for unfiltered access are case sensitive.

Enter the URL of the page you have created in the When entering these addresses you should not enter http:// before the address.

"Consent Accepted" URL (Filtering Off)

When users accept the terms outlined in the Consent page and choose to access the Internet without the protection of filtering, they are shown a page to confirm their selection. Type the URL of this page in the *"Consent Accepted" URL (Filtering Off)* box.

"Consent Accepted" URL (Filtering On)

When users accept the terms outlined in the Consent page and choose to access the Internet with the protection of filtering, they are shown a page to confirm their selection. Type the URL of this page in the *"Consent Accepted" URL (Filtering On)* box.

Mandatory Filtered IP addresses

When users begin an Internet session on a computer where filtering is mandatory, as described below, they are shown a consent page.You create this page, and can add the text from the Acceptable Use Policy, and notification that violations of the AUP are blocked and logged.

Consent Page URL (Mandatory Filtering)

When users access a page that you include in the list of Mandatory Filtered IP Addresses the user is shown a page to inform them that the page is Filtered. Type the URL of this page in the *Consent page URL (Mandatory Filtering* field.

You must include a link in this page to:
`192.168.1.254/iAcceptFilter.html`

If you have changed the IP address or the Firewall use the IP Address of the Firewall instead of **`192.168.1.254.`**

Click the *Update button* to save your changes.

The link for filtered access is case sensitive.

Add New Address

You can configure the Firewall to provide filtering always for certain computers on the LAN. Type the IP addresses of these computers in the *Add New Address* box and click *Submit*. You can add up to 128 IP addresses. To remove a computer from the list of computers to be filtered, highlight the IP address in the list and click *Delete Address.*

To filter individual users by IP address you must use static IP addressing.

6 USING THE FIREWALL DIAGNOSTIC TOOLS

This chapter describes the commands and options available in the *Log* menu and the *Tools* menu. Each menu is broken up into sections shown in the user interface as tabs.

To access a command click on either *Log* or *Tools* on the left hand side of the screen and then on the appropriate tab.

This following sections are covered in this chapter:

- Logs and Alerts
- Viewing the Log
- Changing Log and Alert Settings
- Generating Reports
- Restarting the Firewall
- Managing the Firewall Configuration File
- Upgrading the Firewall Firmware

Logs and Alerts

The Firewall maintains an event log, which contains events that may be security concerns. You can view this log with a browser using the Firewall Web interface or you can set up a tab-delimited text file to be sent automatically and periodically to any e-mail address for convenience and archival purposes.

If you want to be alerted of high-priority information, such as an attack on a server, you can specify that this information is immediately e-mailed, either to the main e-mail address used by the log, or to a different address, such as a paging service.

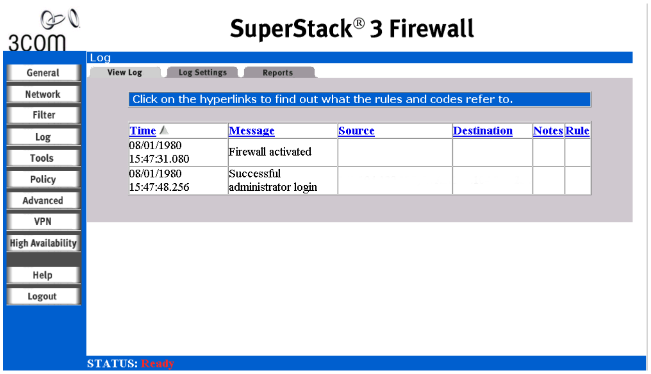
The Firewall logs the following events:

- Unauthorized connection attempts
- Blocked Web, FTP and Gopher sites, and blocked NNTP Newsgroups
- Blocked ActiveX and Java
- Blocked Cookies and Proxy attempts
- Attacks such as IP spoofing, Ping of Death, SYN flood
- Administrator logins
- Successful/unsuccessful loading of the Web Site Filter

Viewing the Log

To view the log click *Log* and then select the *View Log* tab. A window similar to that in Figure 34 displays.

Figure 34 View Log Window



Click on the hyperlinks to find out what the rules and codes refer to.

Time	Message	Source	Destination	Notes	Rule
08/01/1980 15:47:31.080	Firewall activated				
08/01/1980 15:47:48.256	Successful administrator login				

STATUS: Ready

The log is usually displayed as a list in a table, but may appear differently depending on the browser used. You may have to adjust the browser's font size and other viewing characteristics to display the log data most efficiently. Depending on the browser, you can copy entries from the log and paste them into documents. Alternatively, use the *E-mail Log* function and review the log with an e-mail client rather than with a Web browser.

Each log entry contains the date and time of the event, and a brief message describing the event. Some entries contain additional information. Much of this information refers to the Internet traffic passing through the Firewall.

TCP, UDP, or ICMP packets dropped

These log messages describe all traffic blocked from the Internet to the LAN. The source and destination IP addresses of the packet is shown. If the packet was TCP or UDP, the port number, in parentheses, follows each address. If the packet was ICMP, the number in parentheses is the ICMP code. The address information is usually preceded by the name of the service described by either the TCP or UDP port, or the ICMP type in quotation marks.

Web, FTP, Gopher, or Newsgroup blocked

The LAN IP and Ethernet addresses of a machine that attempted to connect to the blocked site or newsgroup is displayed. In most cases, the name of the site which was blocked will also be shown. In addition, there is a box labeled *Rule* which contains one or more lowercase letters. These correspond to the categories in the Web Site Filter as follows:

a = Violence/profanity
b = Partial nudity
c = Full nudity
d = Sexual acts
e = Gross depictions
f = Intolerance
g = Satanic/cult
h = Drug culture
i = Militant/extremist
j = Sex education
k = Gambling/illegal
l = Alcohol/tobacco

See Chapter 11 for more information about these categories.

ActiveX, Java, or Code Archive blocked

The IP addresses of the source machine and the destination server is shown.

When ActiveX or Java code is compressed into an archive it is not always possible to differentiate between the two. If either ActiveX or Java blocking is enabled, all code archives are blocked.

Cookie blocked

The IP addresses of the local machine and the remote server are shown.

Ping of Death, IP Spoof, and SYN Flood Attacks

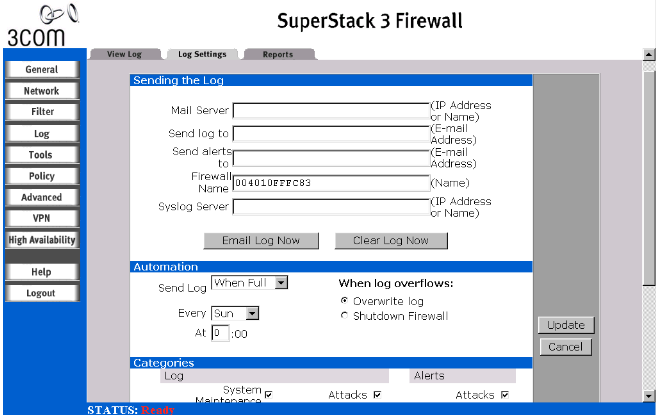
The IP address of the destination machine which may be under attack, as well as the source address which appears in the packet are shown. In these attacks, the source address shown is usually fake and usually cannot be used to determine the source of the attack.

Varying conditions on the Internet can produce conditions which may cause the appearance of an attack, even when no-one is deliberately attacking one of the machines on the LAN or DMZ. This is particularly true for SYN Flood attacks. If the log message calls the attack "possible", or it only happens on an irregular basis, then there is probably no attack in progress. If the log message calls the attack "probable", contact the ISP to see if they can track down the source of the attack. In either case, the LAN and DMZ are protected and you do not need to take further steps.

Changing Log and Alert Settings

Click *Log* and then select the *Log Settings* tab. A window similar to that in Figure 35 displays.

Figure 35 Log Settings Window



Sending the Log

Mail Server (IP Address or Name)

Send log to (E-mail Address)

Send alerts to (E-mail Address)

Firewall Name 004010FFFC83 (Name)

Syslog Server (IP Address or Name)

Automation

Send Log When Full

Every Sun

At 0 :00

When log overflows:

● Overwrite log

○ Shutdown Firewall

Categories

Log

System Maintenance ☑

Attacks ☑

Alerts

Attacks ☑

STATUS: Ready

Sending the Log

Use the Sending the Log feature to inform your administrator of the performance of the Firewall and to make sure that the log file always has space for new entries.

Mail Server

To enable sending log or alert messages via e-mail, you must specify the numerical IP address or the name of your SMTP server. You can obtain this information from the Internet Service Provider that you use to connect the network to the Internet. If you leave this box blank, log and alert messages are not sent via e-mail.

Send Log To

This is the e-mail address to which log files are sent and must be a fully qualified address, for example, `username@3Com.com`. Once sent, the log file is cleared from the Firewall's memory. If you leave this box blank, log messages are not sent by e-mail. You can configure the Firewall to check on a weekly basis if new software is available for download. See "Upgrading the Firewall Firmware" on page 92 for more information. If there is a new software release, an e-mail notification is sent to this address.

Send Alerts To

Alerts are events, such as an attack, which may warrant immediate attention. When an event generates an alert, a message is immediately sent to an e-mail account or e-mail pager. Enter the e-mail address, for example, `username@3Com.com`, to which alert messages are sent in this box. This may be a standard e-mail account or, quite often, a paging service. If you leave this box blank, alert messages are not sent by e-mail.

Firewall Name

A unique name for the Firewall. Enter this ID to identify the Firewall when logs and alerts are emailed to the Network Administrator. Use alphanumeric characters for this field. The MAC address of the Firewall is the default value.

Syslog Server

In addition to the standard screen log, the Firewall can write extremely detailed event log information to an external Syslog server. Syslog is an industry standard protocol used for capturing log information for devices on a network. The Firewall's Syslog captures all screen log activity, plus every connection's source and destination IP addresses, IP service, and number of bytes transferred. To support Syslog, you must have an external server running a Syslog daemon on UDP Port 514. Syslog is a standard feature of UNIX.

Enter the Syslog server's IP address in the *Syslog Server* box.

To download the free 3Com Syslog Server visit:

`http://www.3com.com/ssfirewall`

and click the *Syslog Server* link.

The Firewall supports WebTrends Firewall Suite for comprehensive reporting of the firewall. To enable WebTrends reporting, click on the Log button located at the left side of the browser window. Click on the tab labelled Log Settings just underneath the 3Com banner. On the Log Settings page, enter the IP address of the WebTrends server in the Syslog Server field. Click the Update button on the right of the browser window and restart the Firewall for changes to take effect.

E-mail Log Now

Immediately sends the log to the address in the *Send Log To* box and then clears the log.

Clear Log Now

Deletes the contents of the log.

Changing the Log Automation Settings

The Automation time set here determines when the Firewall queries the 3Com server for new firmware. To ease traffic on the network server, this time is randomized.

Send Log

This pop-up menu is used to configure the frequency of log messages being sent as e-mail: daily, weekly, or only when the log is full. If the weekly or the daily option is selected, specify a time of day when the e-mail is to be sent. If the weekly option is selected, then also specify which day of the week the e-mail is to be sent. If the weekly or daily option is selected and the log fills up, it is automatically e-mailed to the *Send Log To* address and cleared.

When log overflows

In some cases, the log buffer may fill up, which can happen if there is a problem with the mail server and the log cannot be successfully e-mailed. By default the Firewall overwrites the log and discards its contents. As a security measure, you can choose to shut down the Firewall, which prevents any further traffic from traveling through without being logged. To do this select *Shutdown Firewall*.

Selecting the Categories to Log

Click the appropriate check box to enable or disable the generation of the following log message categories.

System Maintenance

When enabled, log messages showing general system maintenance activity, such as administrator logins, automatic loading of Web Site Filters, activation and restarting the Firewall, are generated. This is enabled by default.

System Errors

When enabled, log messages showing problems with DNS, e-mail, and automatic Web Site Filter loading are generated. This is enabled by default.

Blocked Web Sites

When enabled, log messages showing Web sites, newsgroups, or other services blocked by the Web Site Filter, by keyword, or for any other reason are generated. This is enabled by default.

Blocked Java, ActiveX, and Cookies

When enabled, log messages showing Java, ActiveX, and Cookies which are blocked by the Firewall are generated. This is enabled by default.

User Activity

When enabled, log messages showing any successful or unsuccessful user logins will be generated. This is enabled by default.

Attacks

When enabled, log messages showing SYN Floods, Ping of Death, IP Spoofing, and attempts to manage the Firewall from the Internet are generated. This is enabled by default.

Dropped TCP

When enabled, log messages showing blocked incoming TCP connections are generated. This is enabled by default.

Dropped UDP

When enabled, log messages showing blocked incoming UDP packets are generated. This is enabled by default.

Dropped ICMP

When enabled, log messages showing blocked incoming ICMP packets are generated. This is enabled by default.

Network Debug

When enabled, log messages showing Ethernet broadcasts, ARP resolution problems, ICMP redirection problems, and NAT resolution problems are generated. This category is intended for experienced network administrators. This is disabled by default.

Alert Categories

Alerts are events, such as an attack, which may warrant immediate attention. When an event generates an alert, a message is immediately sent to the e-mail account defined in the *Send alerts to* box on the *Log Settings* window (see page 82).

Attacks

When enabled, all log entries that are categorized as an *Attack* are generated as an alert message. This is enabled by default.

System Errors

When enabled, all log entries that are categorized as a *System Error* are generated as an alert message. This is enabled by default.

Blocked Web Sites

When enabled, all log entries that are categorized as a *Blocked Web Site* are generated as an alert message. This is disabled by default.

Click *Update* to save your changes.

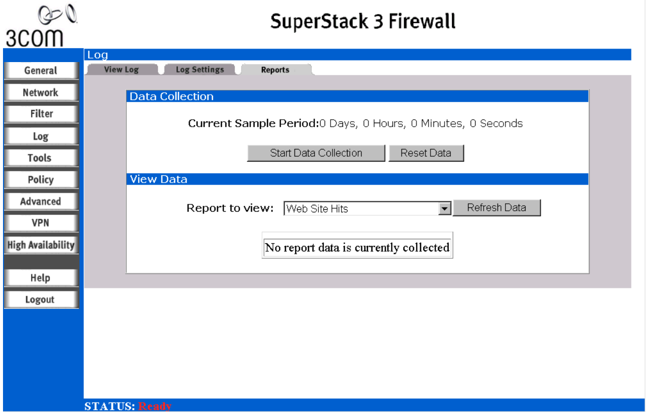
Generating Reports

The Firewall can analyze the event log to show the following:

- Top 25 most accessed Web sites
- Top 25 users of bandwidth by IP address
- Top 25 services that consume the most bandwidth

Click *Log* and then select the *Reports* tab. A window similar to that in Figure 36 displays.

Figure 36 Reports Window



Current Sample Period:0 Days, 0 Hours, 0 Minutes, 0 Seconds

Report to view: Web Site Hits

No report data is currently collected

STATUS: Ready

Collecting Report Data

Start Data Collection

By default, the log analysis function is disabled. Click *Start Data Collection* to begin log analysis. When log analysis is enabled, the button label changes to *Stop Data Collection*.

Reset Data

Click *Reset Data* to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the Firewall is restarted.

Current Sample Period

Displays the current sample period shown in the reports.

Viewing Report Data

Select the desired report from the Display Report popup menu. The options are:

- *Web Site Hits*
- *Bandwidth Usage by IP Address*
- *Bandwidth Usage by Service*.

These reports are explained as follows.

Web Site Hits

Selecting *Web Site Hits* from the *Report to view* drop-down list displays a table showing the URL for the 25 most accessed Web sites and the number of hits to that site during the current sample period.

Use the *Web Site Hits* report to ensure that the majority of Web access is to sites considered applicable to the primary business function. If leisure, sports, or other similar sites are on this list, it may signal the need to change or more strictly enforce the organization's Acceptable Use Policy.

Bandwidth Usage by IP Address

Selecting *Bandwidth Usage by IP Address* from the *Report to view* drop-down list displays a table showing the IP Address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

If using DHCP, remember that the IP address assigned to a computer can change. You may have to check the DHCP server logs to correctly identify which computer is listed in the report.

Bandwidth Usage by Service

Selecting *Bandwidth Usage by Service* from the *Report to view* drop-down list displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio and so forth, and the number of megabytes received from the service during the current sample period.

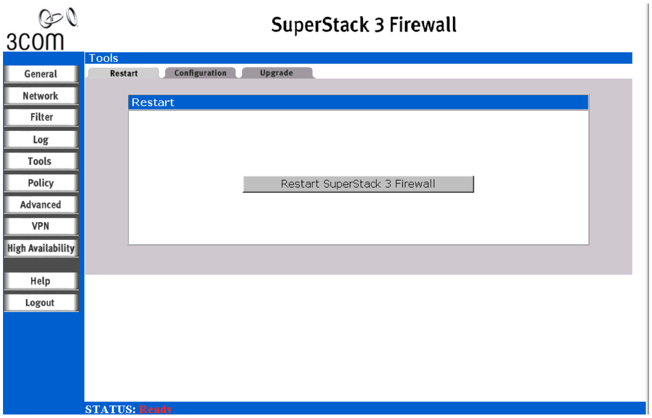
Use the *Bandwidth Usage by Service* report to make sure the Internet services being used are appropriate for the organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, it may signal the need to change or more strictly enforce the organization's Acceptable Use Policy.

Restarting the Firewall

To restart the Firewall:

1 Click *Tools* and select the *Restart* tab. A window similar that in Figure 37 displays.

Figure 37 Restart Window



2 Click *Restart SuperStack 3 Firewall*.

3 Click *Yes* to confirm the restart and send the restart command to the Firewall. The restart takes about 90 seconds, during which time the Firewall cannot be reached from the Web browser and all network traffic through it is halted.

If you have changed the IP settings of the Firewall, you must alter the IP settings of the management station accordingly. You may have to restart the management station, depending on its operating system, for the change to take effect.

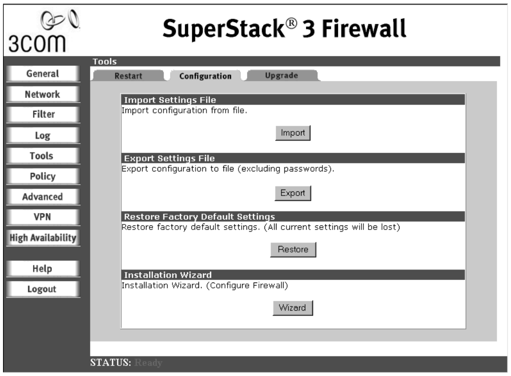
When the Front Panel Power LED stops flashing you can refresh your browser.

To reset the Firewall clearing it of all settings see "Resetting the Firewall" on page 162 for details.

Managing the Firewall Configuration File

The Configuration tool allows you to save and restore the configuration settings of the Firewall. Click *Tools* and then select the *Configuration* tab. A window similar to that in Figure 38 displays.

Figure 38 Configuration Window



Import Settings File
Import configuration from file.

Export Settings File
Export configuration to file (excluding passwords).

Restore Factory Default Settings
Restore factory default settings. (All current settings will be lost)

Installation Wizard
Installation Wizard. (Configure Firewall)

STATUS: Ready

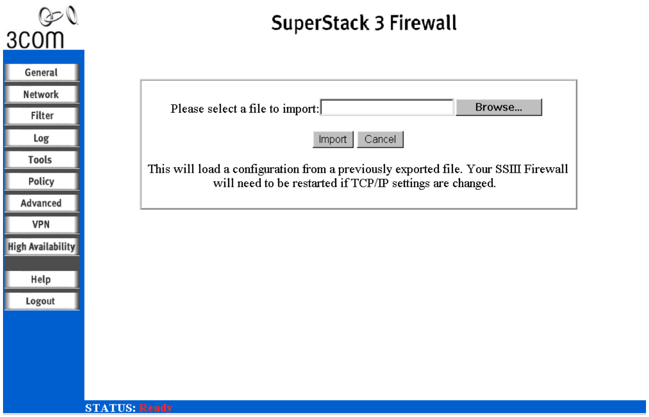
Use the *Configuration* tab to specify where the settings for the Firewall are saved to and retrieved from for backup purposes. You can also restore the default settings from the *Configuration* tab. 3Com recommends that you back up the Firewall settings.

Importing the Settings File

Use this function to import a previously saved settings file back into the Firewall.

1 Click *Import*. A window similar to that in Figure 39 displays.

Figure 39 Import Window



Please select a file to import:

This will load a configuration from a previously exported file. Your SSIII Firewall will need to be restarted if TCP/IP settings are changed.

2 Click *Browse* to find a file which was previously saved using *Export*.

*You may need to set File type to *.* to be able to see the.exp file you exported.*

3 Once you have selected the file, click *Import*.

4 Once the file transfer has completed the status at the bottom of the screen will give you the option to *Restart* the Firewall.

5 Click *Restart*.

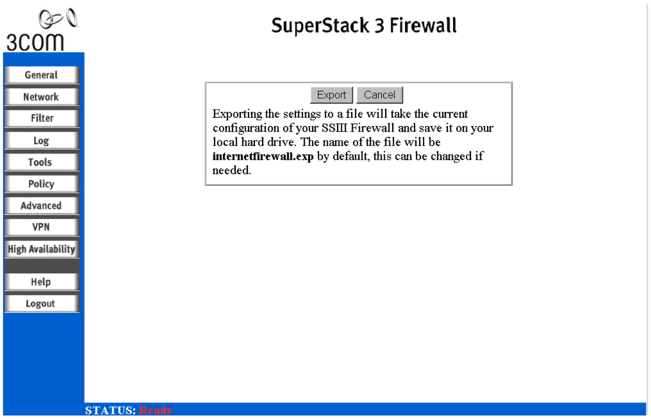
Make sure that the Web browser supports HTTP uploads. If it does not, you cannot import the saved settings.
Note that this will not change the password for the unit.

Exporting the Settings File

You can save the Firewall configuration settings to a file on a local system and then reload those settings.

1 Click *Export*. A window similar to that in Figure 40 displays.

Figure 40 Export Window



Exporting the settings to a file will take the current configuration of your SSIII Firewall and save it on your local hard drive. The name of the file will be **internetfirewall.exp** by default, this can be changed if needed.

STATUS: Ready

2 Choose the location to save the settings file. This should be saved as `<Filename>.exp`. This defaults to `3com_firewall.exp`. The process may take up to a minute.

The Administration password is not saved to the exported file in this process.

Restoring Factory Default Settings

Click *Restore* to clear all configuration information and restore the Firewall to its factory state.

Clicking Restore *will not change the Firewall's LAN IP Address, LAN Subnet Mask, WAN Gateway Address and Password.*

Using the Installation Wizard to reconfigure the Firewall

Click on the Wizard button to start the Installation Wizard. This allows you to configure the Firewall for a new location or role. See Chapter 3, "Quick Setup for the Firewall".

Upgrading the Firewall Firmware

The Upgrade tool allows you to upgrade the operational firmware of the Firewall. The Firewall has flash memory and can be easily upgraded with new firmware.

When upgrading the firmware, all settings will be reset to factory default. 3Com recommends that you export the Firewall's configuration settings before uploading new firmware and then import them again after the upgrade has been completed.

The Firewall checks to see if new firmware is available for download on a weekly basis. If there is a new firmware release, you can configure the Firewall to send an e-mail notification to the address in the *Send log to* box.

Click *Tools* and then select the *Upgrade* tab. A window similar to that in Figure 41 displays.

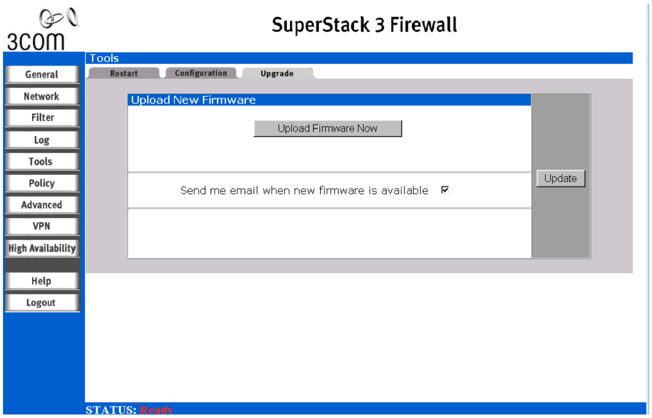
To be notified automatically when new firmware is available:

1 Click the *Send me e-mail when new firmware is available* check box.

2 Click *Update*.

To download new firmware go to **`http://www.3com.com/ssfirewall`** and follow the instructions.

Figure 41 Upgrade Window



Send me email when new firmware is available ☑

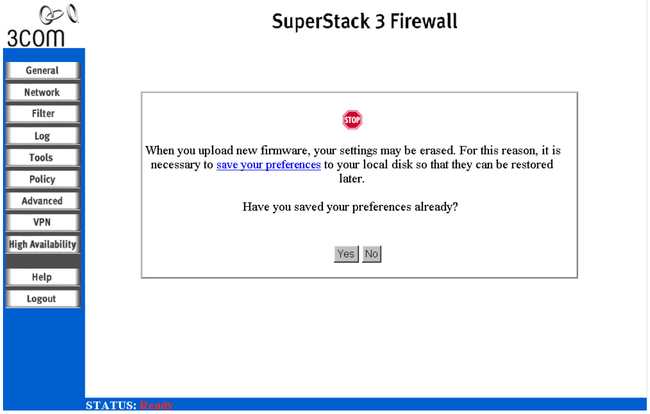
STATUS: Ready

To upload the new firmware onto the Firewall:

1 Click *Upload Firmware Now.*

A window similar to that in Figure 42 displays.

Figure 42 Save Settings Window



SuperStack 3 Firewall

When you upload new firmware, your settings may be erased. For this reason, it is necessary to save your preferences to your local disk so that they can be restored later.

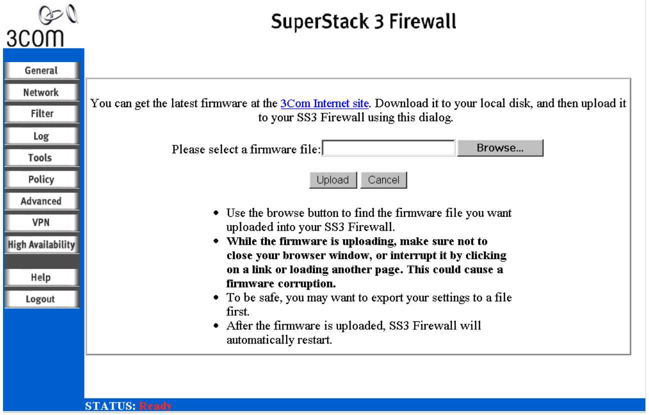
Have you saved your preferences already?

STATUS: Ready

2 Click *Yes* if you have saved the settings.

A window similar to that in Figure 43 displays.

Figure 43 Firmware Upload Window



SuperStack 3 Firewall

You can get the latest firmware at the 3Com Internet site. Download it to your local disk, and then upload it to your SS3 Firewall using this dialog.

Please select a firmware file:

- Use the browse button to find the firmware file you want uploaded into your SS3 Firewall.
- **While the firmware is uploading, make sure not to close your browser window, or interrupt it by clicking on a link or loading another page. This could cause a firmware corruption.**
- To be safe, you may want to export your settings to a file first.
- After the firmware is uploaded, SS3 Firewall will automatically restart.

STATUS: Ready

3 Click *Browse...* and select the firmware file you have downloaded from the 3Com FTP site to a local hard drive or server on the LAN.

4 Click *Upload* to begin the upload.

Make sure that your Web browser supports HTTP uploads.

When uploading the firmware to an Firewall, it is important not to interrupt the Web browser by closing the window, clicking a link, loading a new page, or removing the power to the Firewall. If the Firewall is *interrupted this way, it may result in the Firewall not responding to attempts to log in.*

If your Firewall does not respond, see Chapter 12, "Troubleshooting Guide".

5 Restart the Firewall for the changes to take effect.

7 SETTING A POLICY

This chapter describes the commands and options available in the *Policy* menu. The menu is broken up into sections shown in the user interface as tabs.

To access a command click on *Policy* on the left hand side of the screen and then on the appropriate tab.

This following sections are covered in this chapter:

- Changing Policy Services
- Adding and Deleting Services
- Editing Policy Rules
- Updating User Privileges
- Setting Management Method

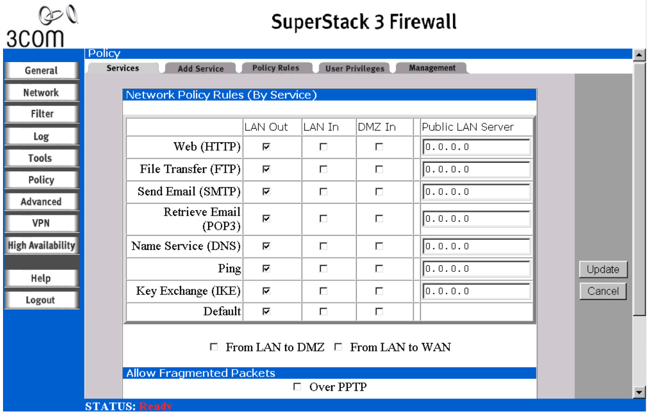
See Chapter 11 for background information about policies.

Changing Policy Services

This section covers which network services are blocked by the Firewall and which are allowed to pass through.

Click *Policy*, and then select the *Services* tab. A window similar to that in Figure 44 displays.

Figure 44 Services Window



Network Policy Rules (By Service)

	LAN Out	LAN In	DMZ In	Public LAN Server
Web (HTTP)	☑	□	□	0.0.0.0
File Transfer (FTP)	☑	□	□	0.0.0.0
Send Email (SMTP)	☑	□	□	0.0.0.0
Retrieve Email (POP3)	☑	□	□	0.0.0.0
Name Service (DNS)	☑	□	□	0.0.0.0
Ping	☑	□	□	0.0.0.0
Key Exchange (IKE)	☑	□	□	0.0.0.0
Default	☑	□	□	

□ From LAN to DMZ □ From LAN to WAN

Allow Fragmented Packets

□ Over PPTP

STATUS: Ready

Amending Network Policy Rules

The *Services* window contains a table showing the defined *Network Policy Rules*. At the bottom of the table is the *Default* rule which affects all IP services. Any rules you create for a specific protocol override the *Default* rule with respect to that protocol.

LAN Out Checkbox

When the check box is clicked for a specific protocol, users on the LAN can access servers of that type on the Internet. When the check box is cleared, users on the LAN *cannot* access servers of that type on the Internet. The default value is enabled. When the *Warning Icon* is displayed to the right of the check box, there is a Custom Rule in the *Rules* tab section that modifies the behavior of the listed Network Access Rule.

LAN In Checkbox

When this check box is cleared, access to the protocol is not permitted from the WAN to the LAN and, if appropriate, from the DMZ to the LAN. When the service is selected, users on the WAN and DMZ can access all hosts on the LAN via that protocol. The default value is disabled; use caution when enabling. When the *Warning Icon* is displayed to the right of the check box, there is a Custom Rule in the *Rules* tab section that modifies the behavior of the listed Network Access Rule. The *LAN In* column is not displayed if NAT is enabled.

DMZ In Checkbox

If you are using the DMZ port on the Firewall access to the protocol is not permitted from the Internet to the DMZ when this check box is cleared. When the service is selected, users on the Internet can access all hosts on the DMZ via that protocol. The default value is enabled. When the *Warning Icon* is displayed to the right of the check box, there is a Custom Rule in the *Rules* tab section that modifies the behavior of the listed Network Access Rule.

Public LAN Server Address

A Public LAN Server is a single host on the LAN that is defined to handle all traffic originating from the Internet to the LAN of a specific protocol, such as HTTP. Define a Public LAN Server by typing its IP address in the *Public LAN Server* box for that protocol. If a server is not designated for a certain protocol, type `0.0.0.0` in the box.

Changing NetBIOS Broadcast Settings

Systems running Microsoft Windows Networking communicate with one another through NetBIOS broadcast packets. By default, the Firewall blocks these broadcasts. If you have Windows computers on more than one port of the Firewall, for example if you are using the Firewall as an internal security measure you may need to enable *NetBios Broadcast Passthrough*.

From LAN to DMZ

To enable Windows machines connected to the LAN port to see other Windows machines connected to the DMZ port in their Network Neighborhood check this box.

Click the *Update* button to save your changes.

From LAN to WAN

To enable Windows machines connected to the LAN port to see other Windows machines connected to the WAN port in their Network Neighborhood check this box.

Click *Update* to save your changes.

NetBIOS passthrough only applies to connections made by using Windows Networking. You will still be able to see web servers using the

HTTP protocol even if both NetBIOS Passthrough boxes are left unchecked.

Enabling Stealth Mode

By default, the Firewall responds to incoming connection requests as either *blocked* or *open*. If you check the box to enable Stealth Mode and click on the *Update* button, no response will be made to inbound requests, which makes your network invisible to potential attackers.

Allowing Fragmented Packets

By default the Firewall drops fragmented packets as they may form part of a Denial of Service attack. Fragmented packets can occur naturally as part of a congested network and you may want to allow them to increase the throughput of your Firewall.

Fragmented packets that are dropped will show as entries in the Firewall Log. See "Viewing the Log" on page 80 for details.

Allow Fragmented Packets over PPTP/IPSec

Point-to-point Tunneling Protocol (PPTP) and IPSec are forms of VPN that allows data to pass through the Firewall without termination. In some cases, passing large amounts of data through the Firewall can cause packets to become fragmented which results in low data throughput.

If fragmented PPTP packets are being blocked check the *Over PPTP* box. If fragmented IPSec packets are being blocked check the *Over IPSec* box.

Setting the Network Connection Inactivity Timeout

If a connection to a server outside the LAN remains idle for more than 5 minutes (default value), the Firewall closes the connection. This is done for security purposes. Without this timeout, it is possible that connections could stay open indefinitely, creating potential security risks. You can increase the timeout interval if users frequently complain of dropped connections in applications such as Telnet and FTP.

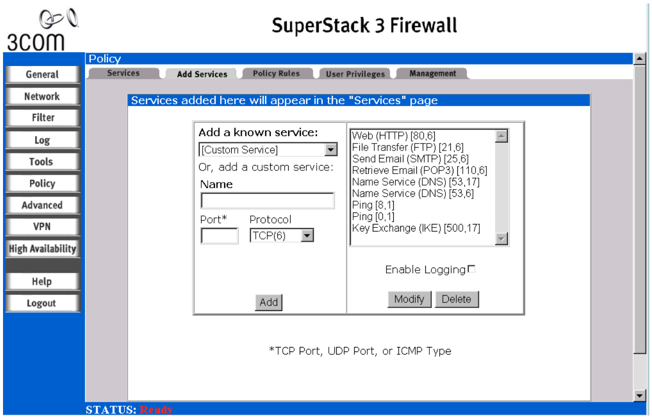
Click *Update* to save your changes.

You must restart the Firewall for these changes to take effect.

Adding and Deleting Services

If a protocol is not listed in the *Services* window, you can add the service. Click *Policy*, and then select the *Add Service* tab. A window similar to that in Figure 45 displays.

Figure 45 Add Service Window



Services added here will appear in the "Services" page

Add a known service: [Custom Service]

Or, add a custom service:

Name

Port*

Protocol TCP(6)

Web (HTTP) [80,6]
File Transfer (FTP) [21,6]
Send Email (SMTP) [25,6]
Retrieve Email (POP3) [110,6]
Name Service (DNS) [53,17]
Name Service (DNS) [53,6]
Ping [8,1]
Ping [0,1]
Key Exchange (IKE) [500,17]

Enable Logging □

*TCP Port, UDP Port, or ICMP Type

STATUS: Ready

The scroll list on the right side of the screen displays all IP protocols that are currently defined and that appear in the *Services* window. Next to the name of the protocol, two numbers appear in brackets. The first number indicates the IP port number which defines the service (either *TCP Port*, *UDP Port,* or *ICMP Type*). The second number indicates the IP protocol type (*6* for TCP, *17* for UDP, or *1* for ICMP).

There may be more than one entry with the same name. For example, the default configuration has two entries labeled Name Service (DNS)*. These are UDP port 53 and TCP port 53. Any entries with identical names are grouped together, and are treated as a single service. Up to 64 entries are supported.*

Adding Support for a Known Service

To add a service known to the Firewall:

1. Select the name of the service from the *Add a known service* drop-down list.
2. Click *Add*.

The new service appears in the list box to the right, along with its numeric protocol description. Note that some well-known services add more than one entry to the list box.

Adding a Custom Service

To add a custom service:

1. From *Add a known service* drop-down list, select *Custom Service*.
2. In the *Name* box, type a unique name, such as **`CC:mail`** or **`Microsoft SQL`**.
3. In the *Port* box, type the IP port number or range of ports.
4. From the *Protocol* drop-down list, select the IP protocol type.
5. Click *Add*.

The new service appears in the list box.

For a list of IP port numbers, see:
`http://www.ietf.org/rfc/rfc1700.txt`

If you create multiple entries with the same name, they are grouped together as a single service and may not function as expected.

Disabling Screen Logs

You can disable the log of events which is usually written to the Firewall's internal Screen Log. For example, if LINUX's authentication protocol is filling the log with entries, you can configure the screen log to ignore all activity for this service. To disable screen logs for a specific service:

1. Highlight the service name in the list box.
2. Clear the *Enable Logging* check box
3. Click *Modify*.

Deleting a Service

To delete a service:

1. Highlight its name in the list box.
2. Click *Delete*.

For services with multiple entries, you can delete only a single Port/Protocol combination from the list. For example, deleting the entry marked *Name Service (DNS) [53,6]* deletes just the TCP portion of the service.

Editing Policy Rules

Network Access Policy Rules evaluate network traffic's source IP address, destination IP address, and IP protocol type to decide if the IP traffic is allowed to pass through the Firewall. Custom rules take precedence, and may override the Firewall's default state packet inspection. Up to 100 policy rules may be entered.

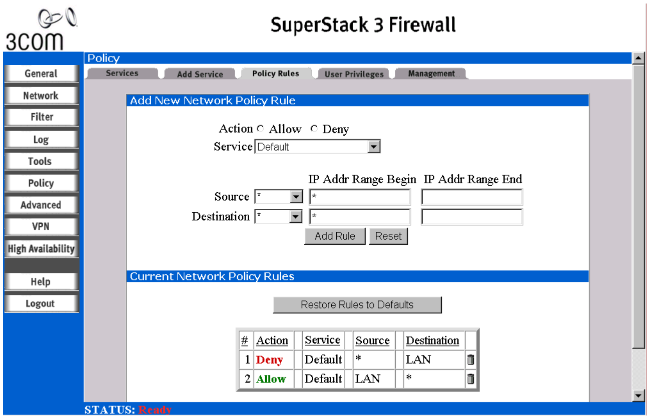
CAUTION: *The ability to define Network Access Rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting Network Access Rules.*

Network Access Rules do not disable protection from Denial of Service attacks, such as SYN Flood, Ping of Death or LAND. However, it is possible to create vulnerabilities to attacks that exploit vulnerabilities in applications, such as WinNuke.

Viewing Network Policy Rules

Click *Policy*, and then select the *Policy Rules* tab. A window similar to that in Figure 46 displays.

Figure 46 Policy Rules Window



Action ○ Allow ○ Deny

Service Default

		IP Addr Range Begin	IP Addr Range End
Source	*	*	
Destination	*	*	

#	Action	Service	Source	Destination	
1	Deny	Default	*	LAN	🗑
2	Allow	Default	LAN	*	🗑

STATUS: Ready

The *Current Network Policy Rules* table is an extension of the *Services* display covered in "Changing Policy Services" on page 97. In this display you will see the default rules and any rules you have created. You can use this screen to fine-tune services and add exceptions.

Rules are arranged in order of precedence from the most specific to the most general.

For example if you block all FTP traffic in one rule and allow a machine with a specific IP address to use FTP in another rule then the second rule will override the first and will be displayed above it.

The table is divided into columns as follows:

Rule Number (#)

Rules are consecutively numbered by precedence and new rules will be inserted into the list by the Firewall at a position appropriate to the breadth of scope of the rule.

When evaluating rules, the Firewall uses the following criteria:

1. A rule defining a specific service is more specific than the default rule.
2. A defined Ethernet link, such as LAN, WAN, or DMZ, is more specific than ***** (all).
3. A single IP address is more specific than an IP address range.

Action

The *Action* for a rule can be set to either *Allow* or *Deny* traffic across the Firewall. For security reasons common protocols are often denied and more specific rules created to describe where these protocols are used legitimately.

Service

The *Service* for a rule shows the service (and hence the protocol) over which the rule operates. A value of *Default* indicates that the rule operates on all traffic. Other values for *Service* are defined in "Adding and Deleting Services" on page 101.

Source

The *Source* of a rule indicates where the connection for that rule is originated. The source can be set to LAN, DMZ, WAN or an specific address or range of addresses on one of those ports.

When a connection is made a two-way conversation is initiated. When allowing a PC on the LAN network port to communicate with a PC or Server on the WAN network port (e.g. to Browse using HTTP) it is unnecessary (and inadvisable) to set a rule for the reverse journey. This *would only be necessary if you wanted the server on the WAN to initiate connections with the PC on the LAN network port.*

Destination

The Destination for a rule refers to the target of the connection made by the source. As with the Source this can be set to a network port specific address or range of addresses.

Time

The *Time* of a Rule shows the hours between which it operates.

Day

The *Day* of a rule shows the days on which it operates.

Enable

The *Enable* checkbox shows whether a rule is currently active. To activate a rule check the checkbox. To deactivate a rule clear the checkbox.

Edit (no column heading)

To Edit the settings for a rule click on the icon of a pencil and paper for the rule you want to edit. Clicking on the icon will bring up the *Edit Rule* window where you can make the changes you need. In the *Edit Rule* window:

- To save your changes click *Update*.
- To leave the Edit Rule window without saving changes close it using the Windows close button.
- To reset all the parameters of the rule to the values they were before you started editing click *Reset*. This will save no changes and will allow you to continue editing.

Delete (no column heading)

To *Delete* the settings for a rule click on the icon of the trash can for the rule you want to edit. Clicking on the icon will bring up a dialog box asking you to confirm the action. Click *OK* to delete the rule. Click *Cancel* if you clicked on the trash can in error.

If you want to stop using a rule which you may want to use again, consider clearing the Enable *checkbox rather than deleting the rule.*

Adding a New Rule

To add a new rule click on the *Add New Rule* button and fill in the fields that you want to change. To keep the field general rather than use a specific value leave the field at its default value.

All fields can be left as default apart from the *Action* field which must have either *Allow* or *Deny* selected.

Restoring Rules to Defaults

To remove all the custom rules click on the *Restore Rules to Defaults* button. This will remove all the custom rule that have been added and will restore the four rules that are implemented as default.

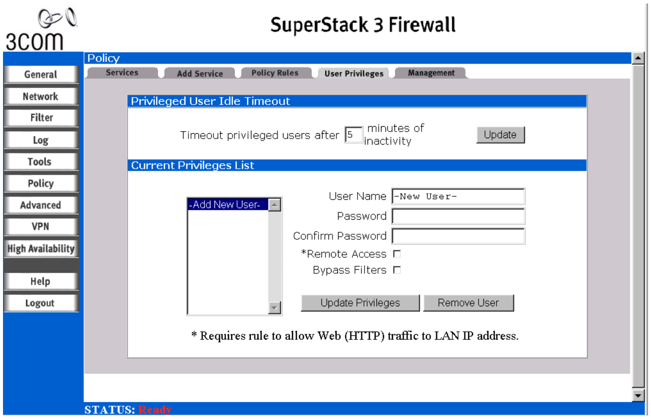
Updating User Privileges

The Firewall provides an authentication mechanism which gives authorized users access to the LAN from remote locations on the Internet as well as a means to bypass the Internet filtering and blocking from the LAN to the Internet. These users are known as *Privileged Users*.

Privileged Users will only be able to use the Services currently allowed by the Firewall. If an external user need full access to your LAN you will need to create a Virtual Private Network (VPN) connection to allow the traffic. See Chapter 9 for instructions on configuring VPN on the Firewall and Chapter 14 for VPN background information.

Click *Policy*, and then select the *User Privileges* tab. A window similar to that in Figure 47 displays.

Figure 47 User Privileges Window



Privileged User Idle Timeout

Timeout privileged users after 5 minutes of inactivity

Current Privileges List

-Add New User-

User Name -New User-
Password
Confirm Password
*Remote Access □
Bypass Filters □

* Requires rule to allow Web (HTTP) traffic to LAN IP address.

STATUS: Ready

Changing the Timeout for Privileged Users

To change the amount of time a privileged user can keep their connection open without using it enter the time in minutes into the *Timeout Privileged Users After* box and click the *Update* button.

The changes made in this dialog box apply to both *Remote Access* users and users that have been allowed to *Bypass Filters*.

Adding Users

To add a new user:

1. Highlight the *Add New User* entry.
2. In the *User Name* box, type the user’s login name.
3. In the *Password* and *Confirm Password* boxes, enter the user’s password.

   It is important to use a password that could not be guessed by someone else. Avoid using names of friends, family, pets, places, and so on. Good passwords can be created by:

   - Making up nonsense words, such as `dwizdell`
   - Including non-alphanumeric ASCII characters in words, such as `so#n&c`

   Passwords are case sensitive.
4. Choose the privileges to be enabled for the user by selecting one or both check boxes.

   Two options are available:

   - *Remote Access*

     Unrestricted access to the LAN from a remote location on the Internet.
   - *Bypass Filters*

     Unrestricted access to the Internet from the LAN, bypassing Web, News, Java, and ActiveX blocking.
5. Click *Update Privileges* to save your changes.

The maximum number of Privileged Users *the Firewall allows is 100.*

User names are not case sensitive; typing **`joe`** *is equivalent to typing* **`JOE`** *or* **`Joe`**. *Passwords* are *case sensitive; typing* **`password`** *is not the same as typing* **`Password`***).*

Changing Passwords and Privileges

To change a user's password or privileges:

1. Highlight the name in the scrollable box.
2. Make the changes.
3. Click *Update User*.

Deleting a User

To delete a user, highlight the name and click *Remove User*.

To configure a user's machine to support privileged users see "Establishing an Authenticated Session" below.

Establishing an Authenticated Session

Authenticated Sessions allow a user on the Internet to access the LAN without restrictions, or allow a user on the LAN to access the Internet without restrictions, bypassing the Web Site Filters.

Make sure that the Web browser software being used to establish an authenticated session support Java, JavaScript or ActiveX scripting.

To establish an Authenticated Session, you point your Web browser at the Firewall's LAN IP Address. This process is identical to the administrator login.

A dialog box is displayed, asking you for the user name and password. After filling in these boxes and clicking *Login*, the password is verified using MD5 authentication. The password is never sent "in the clear" over the Internet, preventing password theft and replay attacks.

Once authenticated, remote users can access all IP resources on the LAN, and users on the LAN can bypass the Web Site Filter. The connection closes if user inactivity on the connection exceeds the configured time-out period. In that case, the remote user must re-authenticate. If it seems like authentication is failing for no reason, make sure that the Caps Lock key on the keyboard is not on.

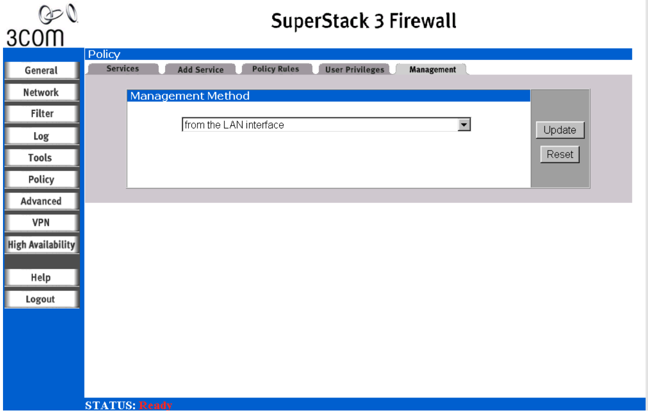
NAT must not be enabled for remote authenticated access.

Setting Management Method

You can manage your Firewall locally, or remotely from a remote host such as a laptop.

Click the button labeled *Policy* on the left side of the browser window and then click the tab labeled *Management* at the top of the window. A window similar to the following displays.

Figure 48 Policy Management Window



Management Method

from the LAN interface

STATUS: Ready

The first step in setting up the management of the Firewall, is selecting the managing method to be used.

- *From the LAN interface* is the default and allows you to manage the Firewall from a web browser on the LAN network. When operating in this mode, no Security Association information is needed.
- *Remotely, from the WAN interface* allows you to manage your Firewall from a remote host. When operating in this mode, you must specify Security Association information so that network traffic between your the Firewall and the remote host is secure. You must also install a VPN Client on the remote host and configure it as follows:

Manage Using Internet Explorer

If you manage the Firewall using Internet Explorer tick the Manage Using Internet Explorer check box. This will allow the Firewall to use Internet Explorer specific code speeding up management.

Click the *Update* button to save your changes.

Selecting Remote Management

When remote management is selected, a Management SA is automatically generated. The Management SA uses Manual Keying to set up a VPN tunnel between the Firewall and the VPN client. The Management SA also defines Inbound and Outbound Security Parameter Indices (SPIs) which match the last eight digits of the Firewall's serial number. The preset SPIs are displayed in the Security Association Information section.

1 Enter a 16 character hexadecimal encryption key in the Encryption Key field or use the randomly generated key that appears in the Encryption Key field. Valid hexadecimal characters are 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E and F. An example of a valid encryption key is:

```
1234567890ABCDEF
```

2 Enter a 32 character hexadecimal authentication key in the Authentication Key field or use the randomly generated key that appears in the Authentication Key field. An example of a valid authentication key is:

```
1234567890ABCDEF1234567890ABCDEF.
```

3 Click the *Update* button and then restart the Firewall for the change to take effect.

Using the Firewall with the NBX 100 Business Telephone System

3Com recommends that you place your NBX 100 Processor on the LAN port of the Firewall. This is to ensure that your telephone system is completely secure from hackers on the Internet.   If you wish to use NBX phones on the WAN or DMZ ports of the Firewall, then you must open a specific port on the Firewall. Do this by following these simple steps:

1 Access the Web interface from a Web browser.

2 Click on the *Policy* button.

3 Click the *Add Service* tab.

4 Type in NBX for the Name of the service.

5 Select UDP for the protocol type and enter 2093 as the Port number.

6 Click *Add*.

7 Click on the *Policy Rules* tab.

8 Click *Allow*, and select NBX from the pull down menu.

9 Click *WAN* or *DMZ* for the Source and select *LAN* for the Destination.

10 Click *Update* and restart the Firewall.

8 ADVANCED SETTINGS

This chapter describes the commands and options available in the *Advanced* menu. The menu is broken up into sections shown in the user interface as tabs.

To access a command click on *Filter* on the left hand side of the screen and then on the appropriate tab.

This following sections are covered in this chapter:

- Automatic Proxy/Web Cache Forwarding
- Specifying Intranet Settings
- Setting Static Routes
- Setting up One-to-One NAT

Automatic Proxy/Web Cache Forwarding

A proxy server intercepts all requests to the Web server to see if it can fulfill the requests by returning a locally stored copy of the requested information. If not, the proxy:

- Completes the request to the server
- Returns the requested information to the user
- Saves it locally to fulfill future requests

Because of this, a proxy can improve Internet response and lessen the load on the Internet link. For example, suppose a school is using the Internet for a research project. A student requests a certain Web page, and then sometime later, a second student requests the same page. Instead of forwarding the request to the Web server where the page resides, the proxy server returns the local copy of the page that it already fetched for the first student.

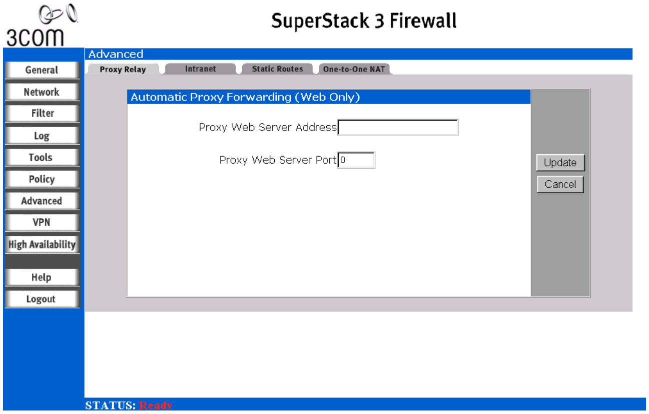
The problem with installing a proxy server on the LAN is that each client must be configured to support the proxy, which adds to administration tasks.

The alternative is to move the proxy to the WAN or DMZ, depending upon the level of protection desired, and enable Automatic Proxy Forwarding. The Firewall can automatically forward all Web proxy requests to the proxy server without client configuration. As a result, no client configuration is required when a Web Proxy is used.

The Firewall can also be used to forward all Web (HTTP) traffic to a Web Cache on the network. The Web Cache can be placed either on the WAN or the DMZ side of the Firewall. The installation is the same as for a Proxy Server. See below.

1 Click *Advanced*, and then select the *Proxy Relay* tab. A window similar to that in Figure 49 displays.

Figure 49 Proxy Relay Window



Automatic Proxy Forwarding (Web Only)

Proxy Web Server Address

Proxy Web Server Port 0

STATUS: Ready

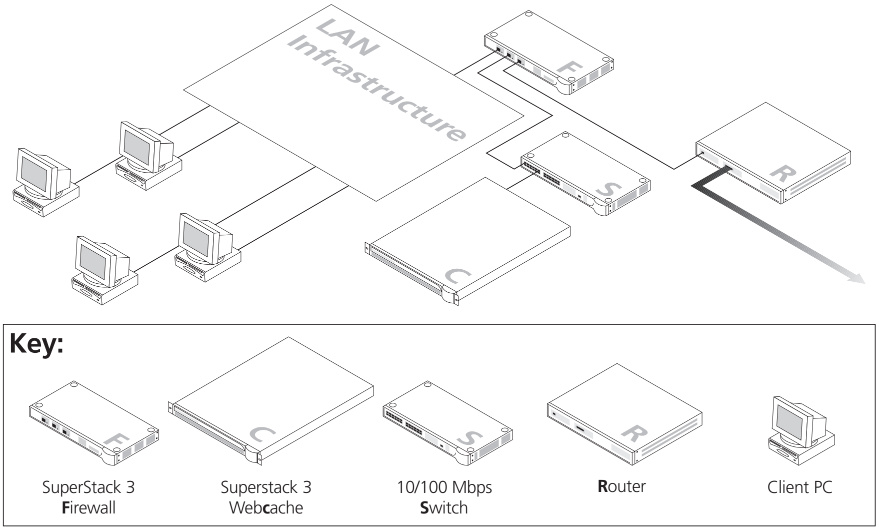
2 Enter the IP address of the proxy in the *Proxy Web Server Address* box, and the proxy's IP port in the *Proxy Web Server Port* box.

3 Click *Update* to save your changes.

Deploying the SuperStack 3 Webcache as a Proxy of the Firewall

The following example describes how to install the 3Com SuperStack® 3 Webcache 1000/3000 (3C16115/3C16116) as a proxy server of the SuperStack 3 Firewall (3CR16110-95). A sample network layout is shown in Figure 50 below.

Figure 50 Deploying the Firewall and Webcache together



1 Install the Webcache as described in the Superstack 3 Webcache User Guide (DUA1611-5AAA0x) taking into account any safety information.

a Install the Webcache on a Hub or Switch connected to the DMZ port of the Firewall. Use the LAN port of the Webcache for this connection.

Network Address Translation (NAT) does not apply to the DMZ port of the Firewall so you will need to configure the Webcache with a registered IP address.

b Set the Webcache to *Proxy Mode*. This setting can be made from the *Getting Started Wizard* or by selecting *Device View* -> *System* -> *Caching* -> *Set Caching Mode* from the Web interface.

c In the *Port Number* field enter the number `8080` (this is the default value).

d Do not configure *Web Site Blocking* on the Webcache as the Firewall has more advanced filtering abilities and is able to use the 3Com Web Site Filter (3C16111).

2 Install the Firewall according to the Superstack 3 Firewall User Guide (this guide) taking into account any safety information.

a On the Web interface of the Firewall click *Advanced* then *Proxy Relay*.

b In the *Proxy Web Server Address* field enter the IP address of your Webcache.

c In the *Proxy Web Server Port* field enter the number `8080`

d Click *Update* to save your changes.

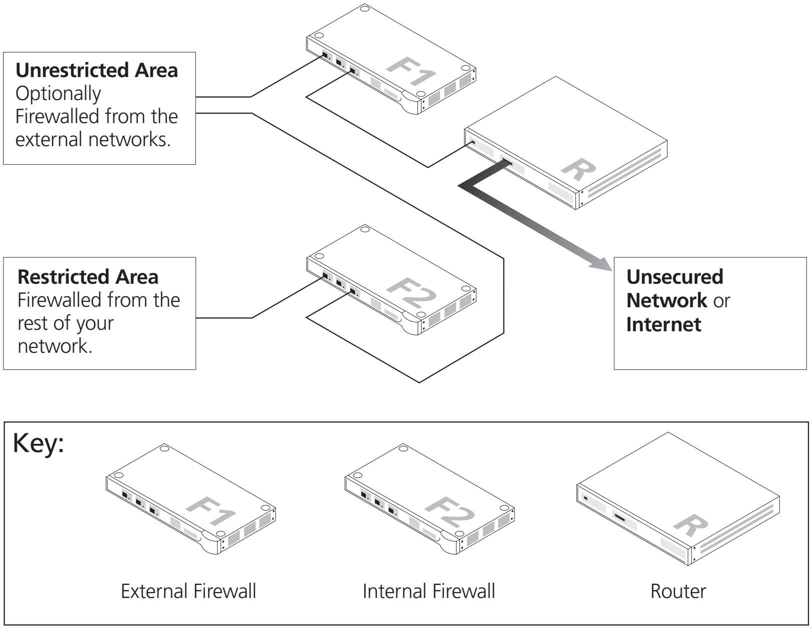
3 No configuration is necessary on the client machines. The Firewall will intercept any HTTP requests for external URLs and will forward the traffic to the Webcache.

Specifying Intranet Settings

In some cases, it is desirable to prevent access to certain resources by unauthorized users on the LAN. For example, a school's administration office may be placed behind the Firewall to restrict access to its computers by users in the Student Computer Lab. Similarly, an organization's accounting, research, or other sensitive resources may be protected against unauthorized access by other users on the same network. By default, protected LAN users can only access the Internet and no other devices between the WAN port and the Internet. To enable access to the area between the Firewall's WAN port and the Internet (referred to as the intranet), you must specify intranet settings for the Firewall.

To achieve internal firewalling, connect a second Firewall between the unrestricted and the restricted segments on the LAN, as shown in Figure 51. In this diagram the Firewall labelled F2 is protecting an internal network.

Figure 51 Connecting the Firewall to protect an internal part of the network


Unrestricted Area
Optionally Firewalled from the external networks.
F1
R
Restricted Area
Firewalled from the rest of your network.
F2
Unsecured Network or Internet
Key:
F1
F2
R
External Firewall
Internal Firewall
Router

Installing the Firewall to Protect the Intranet

The following describes how to install and configure the Firewall to provide intranet firewalling.

1. Connect the Ethernet port labeled LAN on the front of the Firewall to the network segment that will be protected against unauthorized access.
2. Connect the Ethernet port labeled WAN on the front of the Firewall to the rest of the network.

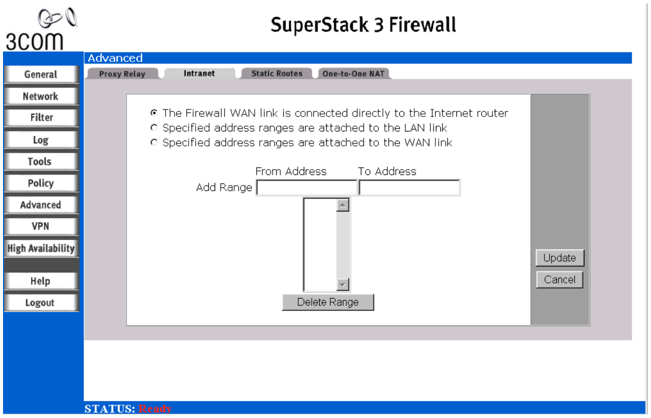
Devices connected to the WAN port do not have firewall or Web Site Filter protection. It is advised that you use another Firewall to protect these computers.

3. Connect the power cord to the back of the Firewall and then connect to an AC power outlet.

Configuring the Firewall to Protect the Intranet

Click *Advanced*, and then select the *Intranet* tab. A window similar to that in Figure 52 displays.

Figure 52 Intranet Window



● The Firewall WAN link is connected directly to the Internet router
○ Specified address ranges are attached to the LAN link
○ Specified address ranges are attached to the WAN link

Add Range — From Address: | To Address:

STATUS: Ready

To enable intranet firewalling, it is necessary to identify which machines are protected against unauthorized access by specifying the IP addresses of these machines. You can do this in two ways:

- Inclusively by specifying which machines are members of the segment with restricted access.
- Exclusively by specifying which machines are not members of the segment with the restricted access.

Using the inclusive method, you specify the IP addresses of the machines which are connected to the Firewall's LAN port. Use this method in cases such as a small accounting office in a large LAN, where it may be easier to identify the small number of machines with restricted access rather than the larger number of machines on the corporate network.

Using the exclusive method, you specify the IP addresses of the machines connected to the Firewall's WAN port. Use this method in cases such as a large school district with a small student computer lab where it would be easier to specify the small number of machines on the WAN which are not protected by the intranet firewall, rather than the larger number of machines which are.

Typically, it is easier to enter the IP addresses from the smaller number of machines. Enter these addresses individually, or as a range.

IP addresses for Workstations on the LAN port must have static IP addresses or use the Internet Firewall as a DHCP server. It is not possible for them to use a DHCP server connected to the WAN port.

- *Firewall's WAN link is connected directly to the Internet router* — Use this setting if the Firewall is protecting the entire network. This is the default setting.

  Click *Update* to save the configuration.
- *Specified address ranges are attached to the LAN link* — Select this when it is easier to specify which devices are on the LAN. If a machine's IP address is not specified, all communications through the Firewall for that machine are blocked.

  Click *Update* to save the configuration.
- *Specified address ranges are attached to the WAN link* — Select this when it is easier to specify which devices are on the WAN port.

  Click *Update* to save the configuration.

Add Range

To enter a range of addresses, such as the 51 IP addresses from `192.168.23.50` to `192.168.23.100`, type the starting address in the *From Address* box and the ending address in the *To Address* box. To specify an individual address, type it in the *From Address* box only. You can specify up to 64 address ranges.

Click the *Update* button to save the configuration.

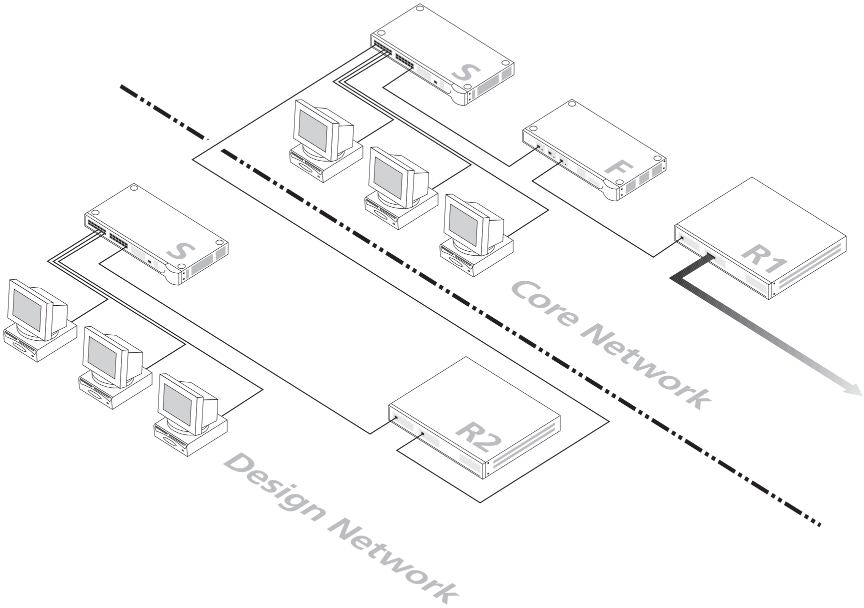
Setting Static Routes

If the LAN has internal routers, you must specify their addresses and network information.

Use static routes if the LAN is segmented into subnets, either for size or practical considerations. For example, you can create a subnet which only contains an organization's graphic design shop, isolating it from traffic on the rest of the LAN.

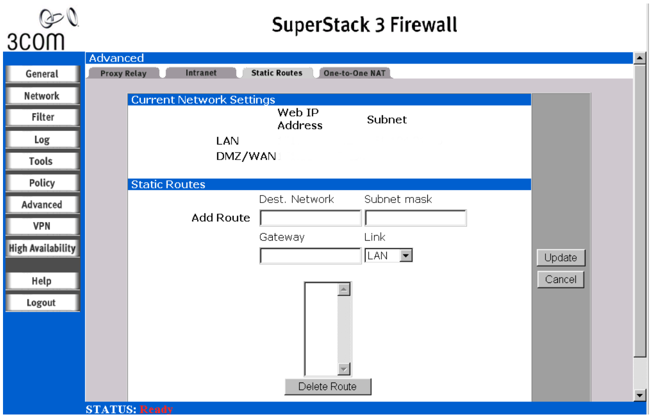
This example is shown in Figure 53 below. Traffic on each network is separated. PCs on the design shop network communicate with PCs on the core network via router *R2*. PCs on the core network communicate with PCs on the design network via the Firewall *F* then the router *R2*.

Figure 53 Isolating a network using a second router



To configure static routes click *Advanced* and then select the *Static Routes* tab. A window similar to that in Figure 54 displays.

Figure 54 Static Routes Window



Current Network Settings

	Web IP Address	Subnet
LAN		
DMZ/WAN		

Static Routes

Add Route — Dest. Network: , Subnet mask:
Gateway: , Link: LAN

STATUS: Ready

LAN

The IP Address and Subnet on the Firewall's LAN port are shown at the top of the window. See "Specifying the LAN Settings" on page 57 to change these settings.

DMZ/WAN

The IP addresses of the DMZ, if appropriate, and WAN ports are shown. These differ from that of the LAN port if NAT is enabled. See "Specifying the WAN/DMZ Settings" on page 58 to change these settings.

Add Route

Type the destination network of the router in the *Dest. Network* box, and the IP address of the router as it appears on Firewall's subnet in the *Gateway* box. From the Link drop-down list, select the port on the Firewall, *LAN* or *WAN*, that the router is connected to. You may have to check the configuration of the LAN routers in order to find this information.

Click *Update* to send the configuration data to the Firewall.

Setting up One-to-One NAT

One-to-One NAT creates a relationship which maps valid external addresses to internal addresses hidden by NAT. Machines with an internal address may be accessed at the corresponding external valid IP address.

To create this relationship between internal and external addresses, define internal and external address ranges of equal length. Once you have defined that relationship, the machine with the first internal address is accessible at the first IP address in the external address range, the second machine at the second external IP address, and so on.

Consider a LAN for which the ISP has assigned the IP address range from `209.19.28.16` to `209.19.28.31`, with `209.19.28.16` used as the NAT Public Address. You have configured the address range of `192.168.1.1` to `192.168.1.255` to be used for the machines on the LAN. Typically, only machines that have been designated as Public LAN Servers are accessible from the Internet. However, with One-to-One NAT, the machines with the internal IP addresses of `192.168.1.2` to `192.168.1.16` can be made accessible at the corresponding external IP address, as shown in Table 4.

Table 4 Address Correspondence in One-to-One NAT

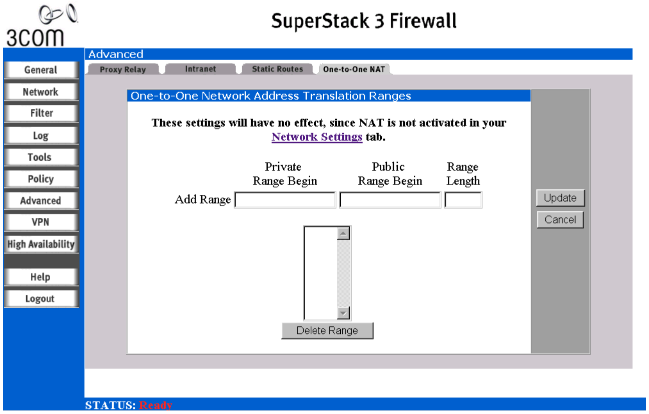
LAN Address	Corresponding WAN Address	Accessed Through
192.168.1.1	209.19.28.16	Inaccessible: Firewall WAN IP Address
192.168.1.2	209.19.28.17	209.19.28.17
[...]	[...]	[...]
192.168.1.16	209.19.28.31	209.19.28.31
192.168.1.17	No corresponding valid IP address	Inaccessible except as Public LAN Server
[...]	[...]	[...]
192.168.1.255	No corresponding valid IP address	Inaccessible except as Public LAN Server

You cannot include the Firewall WAN IP Address in a range.

To set up One-to One NAT click *Advanced*, and then select the *One-to-One NAT* tab. A window similar to that in Figure 55 displays.

Ensure that NAT is enabled before configuring One-to-One NAT. See "Setting the Network Addressing Mode" on page 56 for details.

Figure 55 One-to-One NAT Window



These settings will have no effect, since NAT is not activated in your Network Settings tab.

	Private Range Begin	Public Range Begin	Range Length
Add Range			

STATUS: Ready

Private Range Begin

Type the beginning IP address of the private address range being mapped in the *Private Range Begin* box. This is the IP address of the first machine being made accessible from the Internet.

Do not include the Firewall WAN IP Address in any range.

Public Range Begin

Type the beginning IP address of the public address range being mapped in the *Public Range Begin* box. This address is assigned by the ISP.

Range Length

Type the number of IP addresses for the range. The range length may not exceed the number of valid IP address. You can add up to 64 ranges. To map a single address, use a *Range Length* of 1.

Click *Update* to save changes. Restart the Firewall for changes to take effect.

One-to-One NAT does not change the way the firewall functions work. Access to machines on the LAN from the Internet is not allowed unless you have set up Network Access Rules, or established Authenticated User sessions.

9 CONFIGURING VIRTUAL PRIVATE NETWORK SERVICES

This chapter describes the commands and options available in the *VPN* menu. The menu is broken up into sections shown in the user interface as tabs.

To access a command click on *VPN* on the left hand side of the screen and then on the appropriate tab.

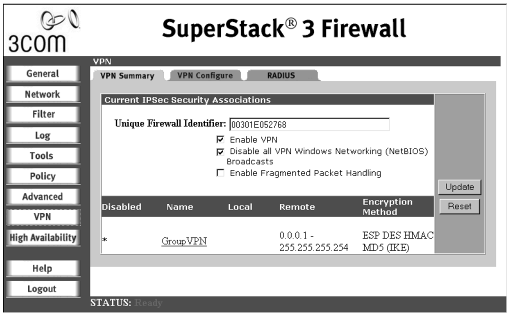
This following sections are covered in this chapter:

- Editing VPN Summary Information
- Configuring a VPN Security Association
- Configuring the Firewall to use a RADIUS Server
- Using the Firewall with Check Point Firewall-1
- Configuring the IRE VPN Client for use with the Firewall

Editing VPN Summary Information

To view the VPN Summary click on *VPN* and then select the *VPN Summary* tab. A window similar to that in Figure 56 displays.

Figure 56 VPN Summary Window



Current IPSec Security Associations

Unique Firewall Identifier: 00301E052768

☑ Enable VPN

☑ Disable all VPN Windows Networking (NetBIOS) Broadcasts

☐ Enable Fragmented Packet Handling

Disabled	Name	Local	Remote	Encryption Method
*	GroupVPN		0.0.0.1 - 255.255.255.254	ESP DES HMAC MD5 (IKE)

STATUS: Ready

Changing the Global IPSec Settings

The Firewall's security uses the IPSec protocol to transmit encrypted data. The settings in the *Current IPSec Settings* section affect all traffic transmitted across the Firewall.

Unique Firewall Identifier

The *Unique Firewall Identifier* is used to identify the Firewall within a network. To change the value enter a string of numbers and letters in the *Unique Firewall Identifier* field and click *Update*. The *Unique Firewall Identifier* defaults to the serial number of the Firewall.

CAUTION: *The* Unique Firewall Identifier *must be different for each Firewall within your network as VPN connections may refer to Firewalls by name.*

Enable VPN

To enable VPN connections check the *Enable VPN* checkbox and click the *Update* button. If VPN is disabled the VPN settings will still be visible on screen and can still be amended but will have no effect until VPN is enabled.

Disable all Windows Networking (NetBIOS) Broadcasts

NetBIOS broadcasts are used when Windows PCs browse their local network. Disabling NetBIOS broadcasts will stop Windows PCs from being able to browse networks on other sites that are connected by the Firewall but will have no effect on browsing the local site or making connections between sites.

Check the *Disable all Windows Networking (NetBIOS) Broadcasts* check box to disable NetBIOS traffic. Click the *Update* button to save your changes.

Enable Fragmented Packet Handling

Check the *Enable Fragmented Packet Handling* box to allow the Firewall to reduce that packet size when communicating with other Firewalls. Enable this check box if "Fragmented IPSec packet dropped" messages appear in the Event Log. Click the *Update* button to save your changes.

Viewing the Current IPSec Security Associations

The *Current IPSec Security Associations* section of the VPN *Summary* screen shows all Security Associations (SAs) that have been created in the VPN *Configure* window. The *Name* listed in the summary table links to the corresponding VPN configuration.

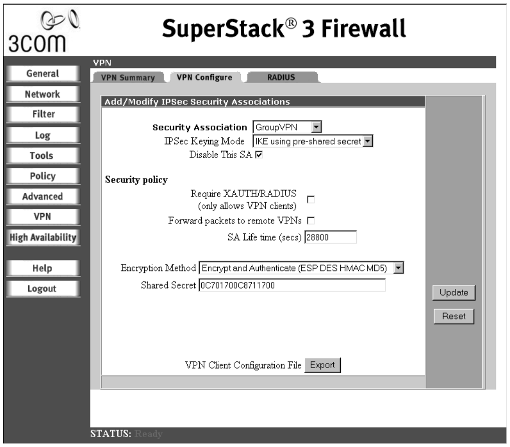
A *Renegotiate* button will appear next to an IKE VPN Security Association when the VPN connection is active. Click the *Renegotiate* button to initiate the VPN handshake and the exchange of new encryption and authentication keys.

The SuperStack 3 Firewall will support 1000 SAs. Of these SAs, 999 will support a single VPN tunnel, while the remaining single SA can support up to 100 concurrent VPN tunnels. This is called the "GroupVPN" SA.

Configuring a VPN Security Association

To configure the VPN Security Associations click on *VPN* and then select the *Configure* tab. A window similar to that in Figure 57 displays.

Figure 57 VPN Configure Window



Add/Modify IPSec Security Associations

Security Association: GroupVPN
IPSec Keying Mode: IKE using pre-shared secret
Disable This SA ☑

Security policy

Require XAUTH/RADIUS (only allows VPN clients) ☐
Forward packets to remote VPNs ☐
SA Life time (secs): 28800

Encryption Method: Encrypt and Authenticate (ESP DES HMAC MD5)
Shared Secret: 0C701700C8711700

VPN Client Configuration File

STATUS: Ready

Adding/Modifying IPSec Security Associations

To add a new Security Association (SA) click the drop down box labelled *Security Associations* and select the option labelled *Add New SA*. Set up the new SA using the options below. Click *Update* to save your changes.

To modify a SA click the drop down box labelled *Security Association* and select the SA you want to modify. Change the SA using the options below. When you have completed your changes click the *Update* button to save your changes.

To delete a SA click the drop down box labelled *Security Associations* and select the SA you want to delete. Click the *Delete* button to delete the SA.

The GroupVPN Security Association cannot be deleted.

IPSec Keying Mode

To select the keying mode click on the *IPSec Keying Mode* drop down box and select one of the options.

- *IKE Using pre-shared secret* (Internet Key Exchange using pre-shared Secret) is the default keying mode and offers more security than a *Manual Key*.
- *Manual Key* does not offer as high a level of security as IKE but is compatible with a wider range of VPN devices.

  This option is not available when using *GroupVPN*.

SA Name

Enter a descriptive name for the Security Association in the *SA Name* field. This allows you to identify the link for which this Security Association was created.

The *SA Name* field is not available when using *GroupVPN*.

Disable This SA

Check the *Disable this SA* box to temporarily disable a Security Association. The association will not be deleted but will cease to function until the check box is unchecked.

IPSec Gateway Address

Enter the address of the target of the VPN link in the *IPSec Gateway Address* field. This will typically be the address of another Firewall or a remote client. If the client does not have a fixed IP address leave this field blank.

This field is not available when using *GroupVPN* and should be left blank if you are setting up a SA for VPN clients which do not have a fixed IP address.

Security Policy

The options in the *Security policy* area of the screen relate to the current Security Association being created/modified. A description of each option is listed below.

Require XAUTH/RADIUS (only allows VPN clients)

Check the *Require XAUTH/RADIUS (only allows VPN clients)* box to force VPN clients to be authenticated by a RADIUS (Remote Authentication Dial-In User Service) Server.

See “Configuring the Firewall to use a RADIUS Server” on page 132 for detailed settings.

This setting is not available if the *IPSec Keying Mode* is set to *Manual Key*.

Enable Windows Networking (NetBIOS) broadcast

NetBIOS broadcasts are used when Windows PCs browse their local network. Enabling NetBIOS broadcasts will allow Windows PCs to browse networks on other sites that are connected by the Firewall. It will have no effect on the local sites or connections made between sites.

Leave the *Disable all Windows Networking (NetBIOS) Broadcasts* box unchecked for the *Enable Windows Networking (NetBIOS) broadcast* setting to have effect. See "Disable all Windows Networking (NetBIOS) Broadcasts" on page 124 for details.

Enable Perfect Forward Secrecy

Check the *Enable Perfect Forward Secrecy* check box to change encryption keys during the second stage of VPN negotiation. This feature blocks intruders from decrypting keys by brute force but extends VPN negotiation time.

This setting is not available if the *IPSec Keying Mode* is set to *Manual Key*.

SA Life time (secs)

The *SA Life time (secs)* field allows you to specify the number of seconds you want a Security Association to last before new encryption and authentication keys must be exchanged.

As the connection is temporarily disabled when the keys are renegotiated, a low value (short time) will increase security but may cause inconvenience. The default value for the *SA Life time (secs)* field is 28800 seconds (8 hours).

Enter the number 28800 or your desired value.

This setting is not available if the *IPSec Keying Mode* is set to *Manual Key*.

Incoming SPI and Outgoing SPI

The *Incoming Security Parameter Index (SPI)* and *Outgoing SPI* are two eight digit hexadecimal numbers that identify the Security Association used for the VPN Tunnel. The *Incoming SPI* and *Outgoing SPI* for a SA can be the same but must differ for all other SPIs used on your network

Additionally the values from 00000000 to 000000FF have been reserved by the Internet Engineering Task Force (IETF) and are not allowed for use as an SPI.

Enter your chosen *Incoming SPI* and *Outgoing SPI* in the relevant fields.

If you enter less than eight hexadecimal digits the SPI will be padded with leading zeros. For example SPIs of "F00" and "00000F00" will be treated as equivalent.

The *Incoming SPI* and *Outgoing SPI* are only used when *Manual Keying* is employed. These fields do not appear when using IKE as your *IPSec Keying Mode*.

Encryption Method

The Firewall supports seven encryption methods for establishing a VPN tunnel. These are shown in Table 5 below.

Table 5 Firewall Encryption Methods

Method	Speed	Security	Supported by
Tunnel Only (ESP NULL) provides no encryption or authentication but can be used to access machines at private addresses behind NAT. Can also be used to allow unsupported protocols through the Firewall.	Very Fast	Low	Manual Key, IKE
Encrypt (ESP DES) uses 56 bit DES to provide an encrypted VPN tunnel. Security professionals consider DES to be a very secure encryption method but it will have a significant impact on the data throughput of the Firewall.	Slow	High	Manual Key, IKE
Fast Encrypt (ESP ARCFour) uses 56 bit ARCFour to provide an encrypted VPN tunnel. ARCFour is widely considered to be a secure encryption method.	Medium	Medium	Manual Key, IKE
Encrypt for Check Point (ESP DES rfc1829) uses 56 bit DES as specified in RFC 1829 to provide an encrypted VPN tunnel. This method will provide interoperability with other IPSec VPN gateways, such as Check Point FW-1.	Slow	High	Manual Key, IKE, Check Point FW-1
Encrypt and Authenticate (ESP DES HMAC MD5) uses 56 bit DES to encrypt and HMAC MD5 to authenticate the VPN tunnel.	Very Slow	Very High	GroupVPN, Manual Key, IKE
Strong Encrypt (ESP 3DES) uses 168 bit 3DES to provide an encrypted VPN tunnel. Security professionals consider 3DES to be an extremely secure encryption method.	Extremely Slow	Extremely High	GroupVPN, Manual Key, IKE
Authenticate (AH MD5) provides and unencrypted but authenticated VPN tunnel. This method uses an Authentication Header (AH) to authenticate the data.	Fast	Low	Manual Key, IKE

Select your preferred method from the *Encryption Method* drop-down box.

Shared Secret

A shared secret is a predefined field that the two endpoints of a VPN tunnel use to set up an IKE SA. This field can be any combination of alphanumeric characters with a minimum length of 4 characters and a maximum of 128 characters. Precautions should be taken when delivering/exchanging this shared secret to assure that a third party cannot compromise the security of a VPN tunnel.

Enter your chosen shared secret in the *Shared Secret* field.

This setting is not available if the *IPSec Keying Mode* is set to *Manual Key*.

Encryption Key

The *Encryption Key* is a hexadecimal number that is used to encrypt the VPN tunnel when using *Manual Keying*. The length of the *Encryption Key* is determined by the method of encryption that is used.

- For 56 bit DES the number must be 16 hexadecimal digits long.
- For 56 bit ARCFour the number must be 16 hexadecimal digits long.
- For 168 bit 3DES the number must be 48 hexadecimal digits long.

If the Encryption Key is less than the value stated above it will be rejected by the Firewall. If it is longer than stated then the number will be truncated and the stated number of digits used.

The *Encryption Key* is only used when *Manual Keying* is employed. This field does not appear when using IKE as your *IPSec Keying Mode*.

Authentication Key

The *Authentication Key* is a hexadecimal number that is used to authenticate the users of the VPN tunnel when using *Manual Keying*. The length of the *Authentication Key* is always 32 digits.

If the *Authentication Key* is less than the value stated above it will be rejected by the Firewall. If it is longer than stated then the number will be truncated.

The *Authentication Key* is only used when *Manual Keying* is employed. This field does not appear when using IKE as your *IPSec Keying Mode*.

Setting the Destination Network for the VPN Tunnel

If you are specifying a Security Association for use with VPN clients in addition to the GroupVPN you must specify the Destination Network for the link.

This option does not appear for the GroupVPN SA. This SA allows does not restrict the IP address of the client.

You do not need to configure the destination network if you are configuring a VPN tunnel to a single VPN device such as Firewall. You only need configure this range if you are connecting to a range of devices such as VPN clients.

Adding a New Network Range

To add a new network range click the *Add New Network* button and enter the address range for the network you want to allow in the dialog box displayed.

To enter a non-contiguous range enter the each block of addresses separately.

Deleting a Network Range

To delete a network range click on the icon of the trash can next to the range you want to delete and confirm your decision when asked.

Editing a Network Range

To edit a network range click of the icon of the pencil and paper next to the range you want to edit. Change the range to the desired value and click the *Update* button.

Configuring the Firewall to use a RADIUS Server

The Firewall is capable of using a RADIUS (Remote Authentication Dial-In User Service) server to authenticate VPN users. To configure your Firewall to use a RADIUS server click on *VPN* on the left hand side of the screen and then on the *RADIUS* tab.

Before using RADIUS to authenticate clients enable RADIUS in the Security policy of a Security Association. See "Security Policy" on page 127.

***CAUTION:** The RADIUS server will only authenticate client devices. Do not enable RADIUS if you are authenticating with another Firewall.*

Changing the Global RADIUS Settings

RADIUS Server Retries

Enter the number of times you want the Firewall to attempt to connect to the RADIUS Server in the *RADIUS Server Retries* field. If the RADIUS server does not respond within the specified number of retries, the VPN connection will be dropped. This field may range between 0 and 30. A value of 3 is recommended for a typical network.

RADIUS Server Timeout in Seconds

The *RADIUS Server Timeout in Seconds* field determines the length of time that will elapse before the Firewall attempts to contact the RADIUS server again after a failure. The RADIUS server timeout may range from 0 to 60 seconds. A value of 5 seconds is recommended for a typical network.

Changing RADIUS Server Details

The primary RADIUS server is defined in the RADIUS server section. An optional secondary RADIUS server may be defined if a backup RADIUS server exists on the network.

The process for configuring a primary RADIUS server is described below. If you have a backup or secondary RADIUS server on your network then repeat the process for the *Secondary Server* fields.

Name or IP Address

Enter the DNS name or IP address of your RADIUS server in the *Name or IP Address* field. Using the name of the server allows you to change its address without reconfiguring the Firewall.

Click the *Update* button to save your changes.

Port Number

Enter the UDP port number that your RADIUS server listens on in the *Port Number* field. This information can be found in the documentation that came with your RADIUS server.

The *Steel-Belted RADIUS Server*, for example, is set to listen on port 1645 by default.

Click the *Update* button to save your changes.

Shared Secret

The shared secret of a RADIUS server is a case sensitive alphanumeric string of up to 30 characters that is used to authenticate the Firewall and the RADIUS server. Your RADIUS server may use its administrative password as a shared secret.

Enter the shared secret or administrative password of your RADIUS server in the Shared Secret Field.

Click the *Update* button to save your changes.

When configured for a RADIUS server the Firewall will record both successful and failed User Logins using XAUTH/RADIUS.

Using the Firewall with Check Point Firewall-1

The most common solution to date for preventing unwanted Internet access has been by fortifying the enterprise network against hackers. Often a Firewall is used at the main entrance of the enterprise network, but that is not always enough. Although the “front door” may be secure and monitored, other portals may not be protected as well. Remote offices are often susceptible and place their data and application availability at risk by providing an unguarded “back door” into the network.

Similar technologies are used to protect alternative portals on an enterprise network, remote networks, and to isolate internal segments of a large network from internal threats. Thus it is possible to have firewalls as portals and use Virtual Private Networks (VPNs) between the enterprise network and remote offices.

A VPN provides a secure, encrypted path over the Internet. A VPN should be required for accessing any non-public information over the Internet. Since VPN standards are still evolving, different vendor's implementations are not always fully interoperable. Ideally, a firewall should be adaptable to support all of the VPN products it may encounter, but not all do.

The VPN features of the Firewall provide interoperability with many different vendors. However, a common VPN firewall solution is provided by Check Point Firewall-1. This section details the steps required to configure the IRE VPN Client and the Firewall to work with Check Point Firewall-1.

Configuring the IRE VPN Client

Launch and log into the SafeNet Soft-PK Security Policy Editor application.

1 Check an existing Firewall object and make sure the Encryption Domain includes all objects for any encryption methods in use. Go to the *Encryption* tab and make sure the *Manual IPSEC* encryption algorithm is

selected for Firewall VPN. If *SecuRemote* is used, *FWZ* must also be selected.

2 Create the Remote Object(s). These are the resources behind the remote Firewall (Workstations, Network or Group Objects). Refer to the following example:

- **a** From the *Manage* menu select *Network Objects.*
- **b** Press the *New* button and select *Network*.
- **c** Give the Network Object a unique name: (for example "Firewall-Network")
- **d** Give the Network Object an IP Address Range (for example "10.1.1.0")
- **e** Give the Network Object a Subnet Mask (for example "255.255.255.0")
- **f** Give the Network Object a Comment (optional)
- **g** Select *External* for the Location Option
- **h** Press the *OK* button when finished.

3 For easier management, you should create a group and place all objects that are protected by the remote Firewall in that group.

- **a** Press the *New* button and select the *Group* option.
- **b** Give the *Group* object a unique Name (for example "Encrypt-Firewall")
- **c** Give the *Group* object a Comment (optional)
- **d** Select the objects that are behind the remote Firewall and *Add* them to the group.
- **e** Press the *OK* button when finished.

4 Create a remote Firewall object.

- **a** Press the *New* button and select the *Workstation* option.
- **b** Give the workstation object a unique name (for example "Firewall-Remote").
- **c** Give the workstation object the external IP address of the Remote Firewall (for example "111.111.111.111").
- **d** Give the workstation object a comment (optional).
- **e** Select *External* for the Location.

f Select *Gateway* for the Type.

g Leave the *Firewall-1 Installed* box unchecked.

h Go to the Encryption Tab. Select the *Other* radio button and select the Group or Network the Firewall will be encrypting for.

i Select the encryption method *Manual IPSEC*.

j Press the *OK* button when finished.

5 Create the SPI key(s) needed to synchronize encryption algorithms.

a From the *Manage* menu select the *Keys* option.

b Press the *New* button and select *SPI*.

c Give the SPI value a unique hexadecimal value.

d Give the SPI key a comment (optional).

e Check the *ESP* box and select *DES* as Encryption Algorithm.

f Make sure that the *AH* box is unchecked (ignore any warning.) *Authentication Algorithm* field should be grayed out.

g Enter an Encryption Key (must be 16 hexadecimal characters.) *Authentication Key* field should be grayed out.

The Encryption Key and SPI Key number must match the settings on the remote Firewall for the VPN to work.

6 Now you must create a rule to allow the Check Point Firewall to exchange IPSEC packets with the remote Firewall.

From the *Edit* menu, select *Add Rule*.

This rule should be added below any Client VPN rules (for SecuRemote to work properly) and above the normal resource access rules. The rule should contain both firewall objects (Check Point Firewall-1 and Firewall), the services should be *IPSEC* group and it should be *Accepted*. Logging is optional and should be used to debug any problems.

7 Next you need to add a rule to allow the two networks/groups to send encrypted data to each other.

This rule should follow right after the firewall IPSec packet exchange rule. The rule should contain both the local network/group with the remote network/group. You can limit the services that are allowed to traverse the VPN tunnel. The action for this rule should be “*Encrypt.*”

8 Right click the *Encrypt* action and select *Edit Properties.*

9 Select the *Manual IPSec* and the *Logging* radio buttons.

10 Press the *Edit* button. Select the SPI Key for this VPN Tunnel.

11 Press the *OK* button when finished with the IPSec properties and press the *OK* button when finished with the Encryption properties.

12 From the Policy menu, select *Install* to activate the security policy. The VPN tunnel will function once the remote Firewall has been configured with a corresponding security association.

Configuring the Firewall

1 Go to the *VPN Configure* screen in the Firewall Web interface. Create a Firewall Security Association, using manual key encryption, and name it *Check Point* (any name will work). Do not use the *Allow Remote Clients* checkbox.

2 Enter a valid destination address range (referring to the LAN behind Check Point). Specify the Check Point's external address as the IPSec Gateway address.

3 Select the Encryption Method *Encrypt for Checkpoint (ESP DES rfc1829)*. Make sure the Encryption Key and the SPIs match the values specified in the Check Point screens (The Firewall doesn't need the '0x' prefixes to denote hexadecimal fields like the Check Point does). There is no need for an authentication key.

4 Update the screen and restart Firewall to activate the VPN configuration.

Configuring the IRE VPN Client for use with the Firewall

This section covers the configuration of the Firewall VPN capability and the installation of the IRE VPN Client Software. There are several parts to this process:

- Setting up the GroupVPN Security Association
- Installing the IRE VPN Client Software
- Configuring the IRE VPN Client

Setting up the GroupVPN Security Association

1 Click on *VPN* on the left hand side of the screen and then on the *Summary* tab.

a Ensure that the *Enable VPN* checkbox is ticked.

b Click the *Update* button to save any changes you have made.

2 Click on the *Configure* tab.

a Select *GroupVPN* from the *Security Association* drop-down box.

b Select *IKE using pre-shared secret* from the I*PSec Keying Mode* drop-down box

c Ensure that the *Disable This SA* checkbox is not ticked.

3 If you want to use a RADIUS server to authenticate users tick the *Require XAUTH/RADIUS* checkbox and set up the Firewall for a RADIUS server as detailed in "Configuring the Firewall to use a RADIUS Server" on page 132.

4 If you do not have a RADIUS server or do not wish to use your RADIUS server to authenticate users ensure that the *Require XAUTH/RADIUS* checkbox is not ticked.

5 Set the *SA Life time (secs)* field to 28000.

6 If you want extremely high security select the *Strong Encrypt and Authenticate* option from the *Encryption Method* drop-down box otherwise select *Encrypt and Authenticate*.

7 Enter an alphanumeric string of up to 30 characters into the *Shared Secret* field. As the security of your VPN tunnel depends on the shared secret pick something that cannot easily be guessed such as a string of numbers and letters.

8 Click the *Export* button and save the resulting file to a safe place. Consider this file as one of the keys to your network and keep it in a safe and private place.

9 Click the *Update* button to save the changes you have made.

Installing the IRE VPN Client Software

1 Insert the CD that came with the Firewall into your CD-ROM Drive.

2 Go to the *VPN CLIENT* directory on the CD.s

3 Double-Click `setup.exe` and follow the VPN client Setup program's step-by-step instructions. This product does not require any serial key for installation.

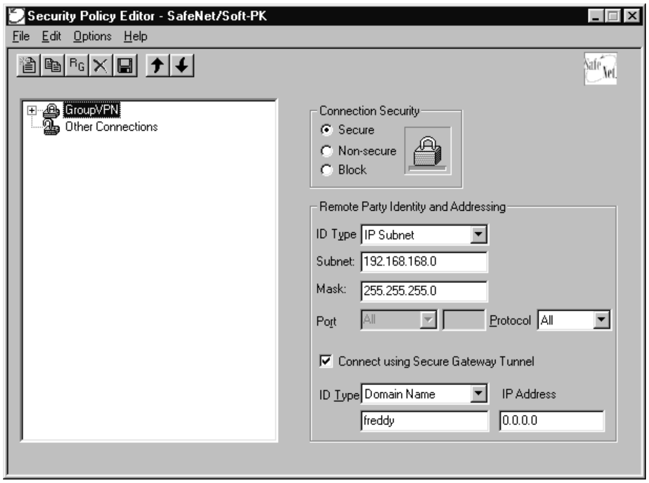
4 Restart your computer after the VPN client Setup program has finished installing.

Configuring the IRE VPN Client

1 Copy the previously saved export file (created in “Setting up the GroupVPN Security Association”) to a floppy disk or to the hard drive of the client machine.

2 Start the Safenet Security Policy Editor. To start the Security Policy Editor either select it from the *SafeNet Soft-PK* submenu of the Windows *Start* menu or double-click the *SafeNet* icon in the toolbar. A window similar to Figure 58 will appear.

Figure 58 Importing a saved *Security Policy*



Connection Security
● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing
ID Type: IP Subnet
Subnet: 192.168.168.0
Mask: 255.255.255.0
Port: All
Protocol: All

☑ Connect using Secure Gateway Tunnel
ID Type: Domain Name
freddy
IP Address: 0.0.0.0

3 Click on the *File* menu and select *Import Security Policy.*

4 Select the exported security file and click the *Open* button.

5. Close the *Security Policy Editor* saving changes when prompted.
6. Delete the export file from the hard drive if it was previously copied there.

   The client is now set up to access your network safely across the Internet.

10 CONFIGURING HIGH AVAILABILITY

This chapter describes the commands and options available in the *High Availability* menu. The menu is broken up into sections shown in the user interface as tabs.

To access a command click on *High Availability* on the left hand side of the screen and then on the appropriate tab.

This following sections are covered in this chapter:

- Getting Started
- Configuring High Availability
- Making Configuration Changes
- Checking High Availability Status
- Forcing Transitions

Getting Started

The High Availability function allows you to connect two Firewalls together as a pair. Although only one Firewall will function at a time the second will automatically take over from the first in the event of a failure.

Before attempting to configure two Firewalls as a High Availability pair, check the following requirements:

- You have two Superstack 3 Firewalls available. The Firewalls must be running the same version of firmware which must be version 6.0 or above.

The 3Com Firewalls 3CR16110-95 and 3CR16110-97 use identical hardware and can be used as a high availability pair provided that they are using the same version of firmware.

- You have at least one static IP address available from your Internet Service Provider (ISP). If you intend to remotely manage both the primary Firewall and the backup Firewall then two addresses are required.

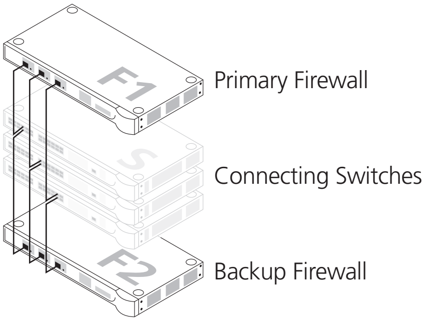
High Availability does not allow the use of dynamic IP address assignment from your ISP.

- Each Firewall in the High Availability pair must have the same upgrades and subscriptions enabled. If the backup unit does not have the same upgrades and subscriptions enabled, these functions will not be supported in the event of a failure of the primary Firewall.

Network Configuration for High Availability Pair

The following diagram illustrates the network configuration for a High Availability pair:

Figure 59 Two Firewalls connected as a High Availability Pair



***CAUTION:** Do not mix the LAN, DMZ and WAN networks when connecting the Firewalls together as this will compromise the security of your network.*

All Firewall ports being used must be connected together with a hub or switch. Each Firewall must have a unique LAN IP Address on the same LAN subnet. If each Firewall has a unique WAN IP Address for remote management, the WAN IP Addresses must be in the same subnet.

The two Firewalls in the High Availability pair will send “heartbeats” over the LAN network segment. The High Availability feature will not function if the LAN ports are not connected together.

Configuring High Availability

Configuring a High Availability pair of Firewalls consists of two steps:

- Configuring High Availability on the Primary Firewall

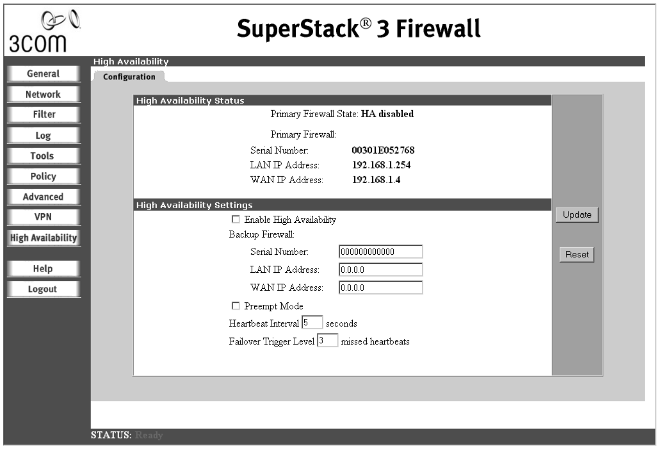
- Configuring High Availability on the Backup Firewall

Both steps must be completed before the two Firewalls will function as a High Availability pair.

Configuring High Availability on the Primary Firewall

Click the *High Availability* button on the left side of the Firewall browser window, and then click the *Configure* tab at the top of the window. A window similar to the following displays.

Figure 60 High Availability Menu



High Availability Status

Primary Firewall State: **HA disabled**

Primary Firewall:

Serial Number: **00301E052768**
LAN IP Address: **192.168.1.254**
WAN IP Address: **192.168.1.4**

High Availability Settings

□ Enable High Availability

Backup Firewall:

Serial Number: 000000000000
LAN IP Address: 0.0.0.0
WAN IP Address: 0.0.0.0

□ Preempt Mode

Heartbeat Interval 5 seconds

Failover Trigger Level 3 missed heartbeats

STATUS: Ready

The top half of the window displays the primary Firewall's serial number and network settings. The bottom half of the window is used to configure High Availability:

1. To enable *High Availability*, check the *Enable High Availability* box.
2. Enter the *Serial Number*, *LAN IP Address* and *WAN IP Address* of the backup Firewall.

The Serial Number and LAN IP Address are required settings for the backup Firewall. The WAN IP Address field may be left blank if remote management is not required for the backup Firewall.

3. Check the *Preempt mode* checkbox to cause the primary Firewall to take over from the backup Firewall whenever the primary is available (for example, after recovering from a failure and restarting).

The primary and backup Firewalls use a "heartbeat" signal to communicate with one another. This heartbeat is sent between the Firewalls over the network segment connected to the LAN ports of the two Firewalls. The interruption of this heartbeat signal triggers the backup Firewall to take over operation from the active unit of the High Availability pair. The time required for the backup Firewall to take over from the active unit depends on the Heartbeat Interval and the Failover Trigger Level.

4 Enter the *Heartbeat Interval* time in seconds. This interval is the amount of time in seconds that elapses between heartbeats passed between the two Firewalls in the High Availability pair.

5 Enter the *Failover Trigger Level* in terms of the number of missed heartbeats. When the backup unit detects this number of consecutive missed heartbeats, the backup Firewall will take over operation from the active unit.

If, for example, the *Heartbeat Interval* and the *Failover Trigger Level* are 5 seconds and 2 missed heartbeats respectively, the backup Firewall will take over from the primary Firewall after 10 seconds in the event of a failure in the primary Firewall.

6 Click the *Update* button. Once the Firewall has been updated, a message confirming the update will be displayed at the bottom of the browser window. If you have modified the *Enable High Availability* setting, you will need to restart the Firewall for change to take effect.

Configuring High Availability on the Backup Firewall

The backup Firewall should not be configured through the Web interface. Instead, configure the backup Firewall by exporting the preferences file from the primary unit and importing the file into the backup unit. This method assures uniform configuration of the two Firewalls in the High Availability pair. To do this:

1 Log into the primary Firewall. Click the *Tools* button on the left side of the browser window and then click the *Configuration* tab at the top of the window. Next, click the *Export* button.

2 Choose a location to save the primary Firewall's preferences file. This file is named "3Com_firewall.exp" by default, but can be renamed. The export process may take up to one minute.

3 Log out of the primary Firewall.

4 Log into the backup Firewall. Click the *Tools* button on the left side of the browser window, and then click the *Configuration* tab at the top of the window. Next, click the *Import* button.

5 Click the *Browse* button and select the file that was previously saved using the Export button. Once the file has been selected, click the *Import* button. Restart the Firewall for the settings to take effect.

The Web browser used to Import Settings must support HTTP uploads.

If the backup Firewall displays an error message when you try to import the preferences file, check for the following problems:

- The firmware version loaded on the backup Firewall does not match the firmware version on the primary Firewall.
- The backup Firewall serial number specified in the primary Firewall's Web interface does not match the actual serial number of the backup Firewall.

To check the backup Firewall firmware version or serial number, click the *General* button on the left side of the browser window and then click the *Status* tab at the top of the window. Both the firmware version and the Firewall serial number are displayed at the top of the window.

In the event of a mismatch in firmware versions, it will be necessary to upgrade the firmware to correct the problem. See "Upgrading the Firewall Firmware" on page 92 for instructions on upgrading firmware.

At this point, you have successfully configured your two Firewalls as a High Availability pair. In the event of a failure in the primary unit, the backup unit will take over operation and maintain the connection between the protected network and the Internet.

Making Configuration Changes

All configuration changes for the High Availability pair must be made on the primary Firewall. Once you have made configuration changes on the primary Firewall, export the updated preferences file and then import the file into the backup Firewall.

Firmware upgrades must be performed separately for the primary and backup Firewalls. See "Upgrading the Firewall Firmware" on page 92 for instructions on upgrading firmware.

Checking High Availability Status

If a failure of the primary Firewall occurs, the backup Firewall will assume the primary Firewall's LAN and WAN IP Addresses. It is therefore not possible to determine which Firewall is active by logging into the LAN IP Address alone.

There are three ways you can check the status of the High Availability pair:

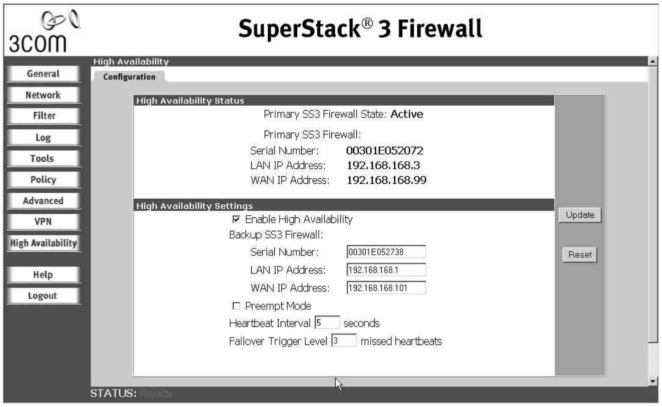
- Check the High Availability Status Window
- Watch for E-mail Alerts.
- View the Log.

These methods are described below.

High Availability Status Window

One method to determine which Firewall is active is to check the High Availability status page for the High Availability pair. To view the High Availability status window, it is necessary to log into the primary Firewall's LAN IP Address. Click the *High Availability* button on the left side of the browser window and then click the *Configuration* tab at the top of the window. If the primary Firewall is active, a window similar to the following will be displayed.

Figure 61 High Availability Status WIndow



High Availability Status

Primary SS3 Firewall State: Active

Primary SS3 Firewall:

Serial Number: 00301E052072
LAN IP Address: 192.168.168.3
WAN IP Address: 192.168.168.99

High Availability Settings

☑ Enable High Availability

Backup SS3 Firewall:

Serial Number: 00301E052738
LAN IP Address: 192.168.168.1
WAN IP Address: 192.168.168.101

☐ Preempt Mode

Heartbeat Interval 5 seconds

Failover Trigger Level 3 missed heartbeats

The first line in the status window above indicates that the primary Firewall is currently Active.

If the backup Firewall has taken over for the primary, for example, in the event of a failure to the primary Firewall, the first line in the status window indicates that the backup Firewall is currently Active.

Check the status of the backup Firewall by logging into the LAN IP Address of the backup Firewall. If the primary Firewall is operating normally, the status window will indicate that the backup Firewall is currently Idle. If the backup has taken over for the primary, this window will indicate that the backup is currently Active.

In the event of a failure in the primary Firewall, you may access the Web interface of the backup Firewall at the primary Firewall's LAN IP Address or at the backup Firewall's LAN IP Address. The primary Firewall will not be accessible until the primary Firewall has become Active again.

E-Mail Alerts Indicating Status Change

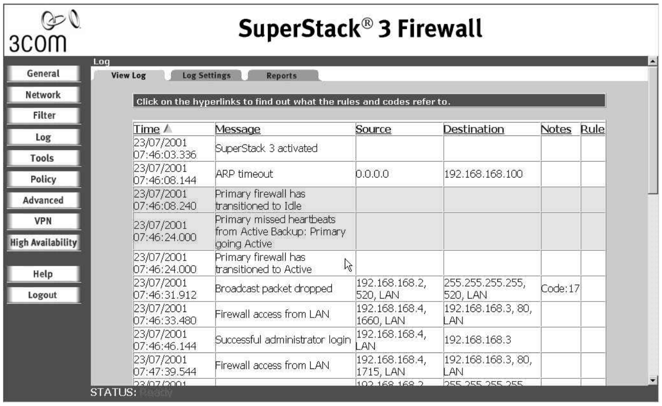
If you have configured the primary Firewall to send e-mail alerts, you will receive an alert e-mail when there is a change in the status of the High Availability pair. For example, when the backup Firewall takes over from the primary after a failure, an e-mail alert will be sent indicating that the backup has transitioned from Idle to Active. If the primary Firewall subsequently resumes operation after that failure, and Preempt Mode has been enabled, the primary Firewall will take over and another E-mail alert will be sent to the administrator indicating that the primary has preempted the backup.

View Log

The Firewall also maintains an event log that displays these High Availability events in addition to other status messages and possible security threats. This log may be viewed with a browser using the Firewall Web interface or it may be automatically sent to the administrator's e-mail address.

To view the Firewall log, click the Log button on the left side of the browser window and then click on the View Log tab at the top of the window. A window similar to the following will be displayed.

Figure 62 Log Screen Showing Switchover of Firewall



Click on the hyperlinks to find out what the rules and codes refer to.

Time	Message	Source	Destination	Notes	Rule
23/07/2001 07:46:03.336	SuperStack 3 activated				
23/07/2001 07:46:08.144	ARP timeout	0.0.0.0	192.168.168.100		
23/07/2001 07:46:08.240	Primary firewall has transitioned to Idle				
23/07/2001 07:46:24.000	Primary missed heartbeats from Active Backup: Primary going Active				
23/07/2001 07:46:24.000	Primary firewall has transitioned to Active				
23/07/2001 07:46:31.912	Broadcast packet dropped	192.168.168.2, 520, LAN	255.255.255.255, 520, LAN	Code:17	
23/07/2001 07:46:33.480	Firewall access from LAN	192.168.168.4, 1660, LAN	192.168.168.3, 80, LAN		
23/07/2001 07:46:46.144	Successful administrator login	192.168.168.4, LAN	192.168.168.3		
23/07/2001 07:47:39.544	Firewall access from LAN	192.168.168.4, 1715, LAN	192.168.168.3, 80, LAN		
23/07/2001		192.168.168.2	255.255.255.255		

Forcing Transitions

In some cases, it may be necessary to force a transition from one active Firewall to another – for example, to force the primary Firewall to become active again after a failure when Preempt Mode has not been enabled, or to force the backup Firewall to become active in order to do preventative maintenance on the primary Firewall.

To force such a transition, it is necessary to interrupt the heartbeat from the currently active Firewall. This may be accomplished by disconnecting the active Firewall's LAN port, by shutting off power on the currently active unit, or by restarting it from the Web interface. In all of these cases, heartbeats from the active Firewall will be interrupted, which will force the currently Idle unit to become Active.

To restart the active Firewall:

1 Log into the primary Firewall's LAN IP Address.

2 Click the *Tools* button on the left side of the browser window.

3 Click the *Restart* tab at the top of the window.

4 Click the *Restart SuperStack 3 Firewall* button, then the *Yes* button to confirm the restart.

Once the active Firewall restarts, the other Firewall in the High Availability pair will take over operation.

⚠ ***CAUTION:*** *If the Preempt Mode checkbox has been checked for the primary Firewall, the primary unit will take over operation from the backup unit after the restart is complete.*

III

ADMINISTRATION AND TROUBLESHOOTING

11 ADMINISTRATION AND ADVANCED OPERATIONS

This chapter provides some background on Firewall concepts and describes some administration functions not available through the menu structure. The following sections are covered in this chapter:

- Introducing the Web Site Filter
- Activating the Web Site Filter
- Using Network Access Policy Rules
- Resetting the Firewall
- Direct Cable Connection

Introducing the Web Site Filter

The 3Com SuperStack 3 Web Site Filter (3C16111) provides the SuperStack 3 Firewall with enhanced Internet filtering capabilities. It can control access from the LAN to thousands of Web sites that might be deemed inappropriate for business use. Twelve selectable Web site categories are provided so Internet access can be tailored to the needs of the organization. Just like the Custom List and filtering by Keywords (see Chapter 8), access to these sites can be enabled or disabled.

The 3Com Web Site Filter is provided as a 12-month subscription, and can be automatically updated weekly to ensure that the filter keeps pace with the ever-changing Internet.

The Firewall comes with a one-month subscription free of charge.

The 3Com Web Site Filter uses the CyberNOT list, which is licensed from The Learning Company. This list is developed and maintained by The Learning Company's Cyber Patrol unit.

The sites on the CyberNOT List are reviewed by a team of Internet professionals, including parents and teachers. They use a set of criteria that categorizes Internet sites and resources according to the level of possibly objectionable content.

In evaluating a site for inclusion in the list, the team consider the effect of the site on a typical twelve year old searching the Internet unaccompanied by a parent or educator. Any easily accessible pages with graphics, text or audio which fall within the definition of the categories below will be considered sufficient to place the source in the category.

- Violence/Profanity:

  Violence: pictures exposing, text or audio describing extreme cruelty, physical or emotional acts against any animal or person which are primarily intended to hurt or inflict pain. Profanity: is defined as obscene words or phrases either audio, text or pictures.

- Partial Nudity:

  Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia. The Partial Nudity category does not include swimsuits (including thongs).

- Full Nudity:

  Pictures exposing any or all portions of the human genitalia. Please note: The Partial Nudity and Full Nudity categories do not include sites containing nudity or partial nudity of a non-prurient nature. For example: web sites for publications such as National Geographic or Smithsonian Magazine or sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.

- Sexual Acts:

  Pictures, descriptive text or audio of anyone or anything involved in explicit sexual acts and or lewd and lascivious behavior, including masturbation, copulation, pedophilia, intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian or homosexual encounters. Also includes phone sex ads, dating services, adult personal ads, CD-ROMs and videos.

- Gross Depictions:

  Pictures, descriptive text or audio of anyone or anything which are crudely vulgar or grossly deficient in civility or which show scatological impropriety. Includes such depictions as maiming, bloody figures, autopsy photos or indecent depiction of bodily functions.

- Intolerance:

  Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

- Satanic/Cult:

  Satanic material is defined as: Pictures or text advocating devil worship, an affinity for evil, or wickedness. A cult is defined as: A closed society, often headed by a single individual, where loyalty is demanded, leaving may be punishable, and in some instances, harm to self or others is advocated.

  Common elements may include: encouragement to join, recruiting promises, and influences that tend to compromise the personal exercise of free will and critical thinking.

- Drugs/Drug Culture:

  Pictures or text advocating the illegal use of drugs for entertainment. Includes substances used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This category does not include material about the use of illegal drugs when they are legally prescribed for medicinal purposes (e.g., drugs used to treat glaucoma or cancer).

- Militant/Extremist:

  Pictures or text advocating extremely aggressive and combative behavior, or advocacy of unlawful political measures. Topics include groups that advocate violence as a means to achieve their goals. Includes: How to, information on weapons making, ammunition making or the making or use of pyrotechnics materials. Also includes the use of weapons for unlawful reasons.

- Sex Education:

  Pictures or text advocating the proper use of contraceptives. This topic would include condom use, the correct way to wear a condom and how to put a condom in place. Also included are sites relating to discussion about the use of the Pill, IUDs and other types of contraceptives. In addition to the above, this category will include discussion sites on how to talk to your partner about diseases, pregnancy and respecting boundaries. The Sex Education category is uniquely assigned; sites classified as Sex Education are not classified in any other category. This permits the user to block or allow the Sex Education category as appropriate, for example, allow the material for an older child while restricting it for a younger child.
  Not included in the category are commercial sites that sell sexual paraphernalia. These sites are typically found in the Sex Acts category.

- Questionable/Illegal & Gambling:

  Pictures or text advocating materials or activities of a dubious nature which may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using someone's phone lines without permission) and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, on-line sports or financial betting, including non-monetary dares and "1-900" type numbers.

- Alcohol & Tobacco:

  Pictures or text advocating the sale, consumption, or production of alcoholic beverages or tobacco products, including commercial sites in which alcohol or tobacco products are the primary focus. Pub and restaurant sites featuring social or culinary emphasis, where alcohol consumption is incidental are not in this category

For further details refer to:
`http://www.cyberpatrol.com`

Activating the Web Site Filter

When you register the Firewall you will be given 30 days free subscription to the Web Site Filter. To continue getting upgrades to the Web Site Filter (covering new Web Sites as they appear) you will need to purchase the annual Web Site Filter subscription.

To activate your annual subscription perform the following steps:

1. Using a Web browser, go to the Firewall registration page
   `http://www.3com.com/ssfirewall/`
2. Click the *Web Site Filter Registration* link.
3. In the box labeled *Serial Numbe*r, type the Internet Firewall's serial number

   The Firewall's serial number is printed on the bottom of the Firewall and is also displayed at the top of the Status window in the Web interface.

4. In the *Activation Key* box, type the key supplied with the Web Site Filter.
5. Click *Activate.*

After a short while, a message confirming the subscription's activation is displayed in the Web browser window.

You must have already registered the Firewall before Activating the Web Site Filter.

Using Network Access Policy Rules

Network Access Policy Rules are the tools you use to control traffic between the LAN, DMZ and WAN ports of your Firewall.

Use this list to help you create rules.

- State the intent of the rule.

  The following are examples of intent for rules:

  - This rule will restrict all IRC access from the LAN to the Internet.
  - This rule will allow a remote Lotus Notes server to synchronize over the Internet to an internal Notes server.
- Is the intent of the rule to allow or deny traffic?
- What is the flow of the traffic: from the LAN to the Internet, or from the Internet to the LAN?
- List which IP services will be affected.
- List which computers on the LAN will be affected.
- List which computers on the Internet will be affected.

The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

Once you have defined the logic of the rule, it is critical to consider the security ramifications created by the rule:

- Will this rule stop LAN users from accessing critical resources on the Internet?

  For example, if IRC is blocked, are there users that require this service?
- Is it possible to modify the rule to be more specific?

  For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- Will this rule allow Internet users access to resources on the LAN in a manner that may create an undue security vulnerability?

  For example, if NetBIOS ports (UDP 137, 138, 139) are allowed from the Internet to the LAN, Internet users may be able to connect to PCs with file sharing enabled.

- Does this rule conflict with any existing rules?

  Once you have answered these questions, to add rules you type the information into the correct boxes in the *Policy Rules* window.

a *Action*

Select the *Allow* or *Deny* option button depending on the intent of the rule, as defined by item 2 in the “Using Network Access Policy Rules” on page 157.

b *Service*

From the *Service* menu, select the IP protocol, as defined by item 4 in the “Using Network Access Policy Rules” on page 157. If the protocol is not listed, it is necessary to first define it in the *Add Service* window.

c *Source*

There are three parameters to configure for the *Source* item.

- Select the Network Access Rule’s source port, *LAN*, *WAN*, or *DMZ*, if appropriate, from the *Ethernet* menu.
- If there are IP address restrictions on the source of the traffic, such as keeping competitors off the company’s Web site, type the starting and ending IP addresses of the range in the *Addr. Range Begin* and *Addr. Range End*, respectively.
- If all IP addresses are affected, type * in the *Addr. Range Begin* box.

d *Destination*

There are three parameters to configure for the *Destination* item.

- Select the Network Access Rule’s destination port, *LAN*, *WAN*, or *DMZ*, if appropriate, from the *Ethernet* menu.
- If there are IP address restrictions on the destination of the traffic, such as limiting Telnet to a remote site, type the starting and ending IP addresses of the range in the *Addr. Range Begin* and *Addr. Range End*, respectively.
- If all IP addresses are affected, type * in the *Addr. Range Begin* box.

Understanding the Rule Hierarchy

The rule hierarchy has two basic concepts:

- Specific rules override general rules.
- Equally specific Deny rules override Allow rules.

When evaluating rules, the Firewall uses the following criteria:

- A rule defining a specific service is more specific than the default rule.
- A defined Ethernet link, such as LAN, WAN, or DMZ, is more specific than ***** (all).
- A single IP address is more specific than an IP address range.

Rules are listed in the Web interface from most specific to the least specific, and rules at the top override rules listed below.

Examples of Network Access Policies

The following examples illustrate methods for creating Network Access Policy Rules.

Blocking LAN Access to Specific Protocols

This example shows how to block all LAN access to NNTP servers on the Internet.

1 For the Action, choose *Deny*.

2 From the *Service* list, choose *NNTP*.

If the service is not listed in the menu, add it in the *Add Service* window.

3 Select *LAN* from the *Source Ethernet* list.

4 Since all computers on the LAN are to be affected, enter * in the *Source Addr. Range Begin* box.

5 Select *WAN* from the *Destination Ethernet* menu.

6 Since the intent is to block access to all NNTP servers, enter * in the *Destination Addr. Range Begin* box.

7 Click *Add Rule*.

Block Access to Specific Users

This example shows how to create a rule which blocks a certain range of computers, such as a competitor, from accessing the public Web server on the LAN or DMZ.

1 For the Action, choose *Deny*.

2 From the *Service* list, choose *HTTP*.

3 Select *WAN* from the *Source Ethernet* list.

4 Enter the blocked network's starting IP address in the *Source Addr. Range Begin* box and the blocked network's ending IP address in the *Source Addr. Range End* box.

5 Select * from the *Destination Ethernet* list.

6 Since the intent is to block access to all servers, enter * in the *Destination Addr. Range Begin* box.

7 Click *Add Rule*.

Enabling the ISP to Ping the Firewall

By default, the Firewall does not respond to pings from the Internet. However, Ping is a tool that many ISPs use to verify that the Internet connection is active.

In this example, you limit the source to allow the ISP to ping the Firewall only.

1 For the Action, choose *Allow*.

2 From the *Service* list, choose *Ping*.

3 Select *WAN* from the *Source Ethernet* list.

4 Enter the starting IP address of the ISP's network in the *Source Addr. Range Begin* box and the network's ending IP address in the *Source Addr. Range End* box.

5 Select *WAN* from the *Destination Ethernet* list.

6 Since the intent is to allow a ping only to the Firewall, enter the Firewall's LAN IP Address in the *Destination Addr. Range Begin* box.

7 Click *Add Rule*.

Restore the Default Network Access Rules

If the Firewall's network access rules have been modified or deleted, the administrator may wish to restore them to the factory default settings. The default rules block all incoming traffic from the WAN to the LAN and allow all outgoing traffic from the LAN to the WAN.

Click the *Restore Rules to Defaults* button at the bottom of the Rules page to restore the default network access rules. A dialog box will display the message, "This will erase all settings you have made on the Services and Rules tab." Click *OK* and restart the Firewall for the changes to take effect.

Restoring the default rules will delete all custom rules and Public LAN Servers. If an IKE VPN Security Association has been created, a service will need to be recreated to permit IKE negotiations.

Protocols/Services to Filter

Although the Firewall is shipped in a safe mode by default, the user can alter the Policy Rules and potentially cause the Firewall to be vulnerable to attacks. Therefore, before any modifications are made, the user should be aware of which services are of most risk to the private LAN.

The following table shows the protocols that are inherently vulnerable to abuse and should be blocked from entering or leaving the site.

Table 6 Protocol Definitions and Characteristics

Protocol Name	Port Number	Risk
TFTP-Trivial FTP	69	This protocol can be used to boot diskless workstations, terminal servers and routers, and can also be used to read any file on the system, if set up incorrectly.
X Windows	6000+	This can leak information from X window displays including all keystrokes.
DNS-Domain Names Service	53	The DNS service contains names of hosts and information about hosts that could be helpful to attackers.
RIP-Routing Information Protocol	520	This service can be used to redirect packet routing.
UUCP-UNIX-to-UNIX CoPy	540	If this service is not properly configured, it can be used for unauthorized access.
Open Windows	2000	This protocol can also leak information about what keystrokes are depressed.
RPC-Remote Call Procedure	111	The RPC services, including NIS and NFS, can be used to steal system information such as passwords and read to write files.
Rexec	512	These protocols can permit unauthorized access to accounts and commands
Rlogin	513	
Rsh	514	
		Other services, whether inherently dangerous or not, should be restricted to only those systems that need them as shown below:

Table 6 Protocol Definitions and Characteristics

Protocol Name	Port Number	Risk
Telnet	23	Restrict to certain systems
FTP-File Transfer Protocol	20,21	Restrict to certain systems
SMTP-Simple Mail Transfer Protocol	25	Restrict to central e-mail server

While some of these services such as TELNET or FTP are inherently risky, blocking access to these services completely may be too drastic a policy for many sites. Not all systems, though, generally require access to all services. For example, restricting TELNET or FTP access from the Internet to only those systems that require the access can improve security at no cost to user convenience.

Services such as NNTP (Network News Transfer Protocol) may seem to pose little threat, but restricting these services to only those systems that need them helps to create a cleaner network environment and reduces the likelihood of exploitation from yet-to-be-discovered vulnerabilities and threats.

Resetting the Firewall

You cannot retrieve a lost administrator password from the Firewall. If you want to reset your Firewall to factory default settings, and can access the Web interface of the Firewall successfully, 3Com recommends that you use the “Restore Factory Defaults” command, described on page 187.

However, if it is no longer possible to access the Web interface (for example, due to a lost password), then you must completely reset your Firewall.

CAUTION: *The reset procedure described below not only deletes all the settings from your Firewall, but also erases the current copy of the firmware from the unit. For this reason, 3Com recommends that you save your firewall settings on a regular basis, and that you also have a copy of the latest firmware available locally. A copy is available on the companion CD to get you up and running again.*

Resetting the Firewall

To reset the Firewall:

1 Disconnect the power from the Firewall.

2 Using a blunt pointed object, fully press in the reset button on the back panel.

3 Whilst holding this button in, reconnect the power to the unit.

4 Continue holding the reset button in until the Alert LED starts flashing. This should be approximately 20 seconds.

5 When the Alert LED stops flashing, the reset is complete. You can now release the reset button.

When the reset is complete, the Firewall restarts. The Power LED stops flashing and the Alert LED is illuminated continuously, indicating that the unit has been reset and the firmware erased.

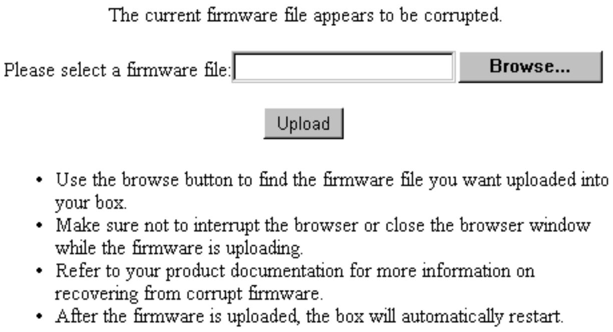
Reloading the Firmware

Even when the firmware has been erased, you can use a basic Web interface to get the Firewall up and running again. The Firewall reverts to its default IP address of 192.168.1.254 after a complete reset, so you must reconfigure your chosen management station to an IP address in the same subnet to access the Web interface.

To reload the firmware:

1 Type **`http://192.168.1.254`** into the web browser on the management station, and press *Enter*. The basic Web interface loads, similar to that shown in Figure 63.

Figure 63 Firmware Upload Window



The current firmware file appears to be corrupted.

Please select a firmware file:

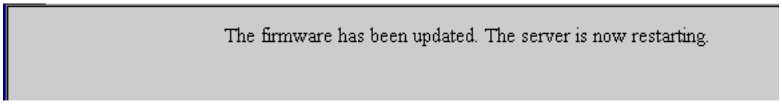
- Use the browse button to find the firmware file you want uploaded into your box.
- Make sure not to interrupt the browser or close the browser window while the firmware is uploading.
- Refer to your product documentation for more information on recovering from corrupt firmware.
- After the firmware is uploaded, the box will automatically restart.

Make sure that you are using the browser that supports HTML uploads, otherwise you cannot upload the firmware.

2 In the box labeled *Please select a firmware file*, type in the full file and path name of the firmware image that you want to upload to the unit. Use the *Browse* button to locate the file if you are not sure of its location.

3 Once you have located the file, click *Upload* to upload the firmware. This process takes approximately one minute. Once complete, the firewall restarts automatically, and the message shown in Figure 64 is displayed.

Figure 64 Firmware Upload Complete



The firmware has been updated. The server is now restarting.

The self-test cycle should now complete successfully. If the entire process has been successful, the power LED should light up and remain on after 90 seconds, and the Alert LED should remain off. You can now access the firmware at the default IP address of 192.168.1.254. The default user name is `admin`, and the default password is `password`.

Once you have logged into the Web interface, you may upload your saved settings file, as described in "Configuration" on page 185. Note that the administrator password is not uploaded, and is still `password` once the upload is complete. Make sure that you change this password to increase the security of the unit.

If you do not have a saved settings file, you must set up the unit from scratch. See Chapter 3 for a quick start guide, Chapter 8 for a complete command reference of the user interface.

Direct Cable Connection

The security of the Firewall is ensured by the use of a secret Administrator Password. Once the password is set, it is used to authenticate the administrator's identity as well as to conceal any important information exchanged with the Web interface. For example, when the administrator's password is changed, the old password is used to conceal the new one.

The Firewall comes pre-configured from the factory with a default password. It is critical to change this password during the initial configuration of the firewall. Unfortunately, the default password can only provide limited protection the first time the administrator's password is set. In principle, an individual inside the network could capture all network transmissions and then perform mathematical analyses to discover the new Administrator Password. Though this is more an academic than a practical issue, using the *Direct Connection* option to set the password for the first time may be advisable if this is a concern.

Direct Connection Instructions

To connect a management station directly to the firewall follow the steps below.

1 Disconnect the management station from the local Ethernet network.

2 Attach the Firewall directly to the management station.

To do this, connect a cable from the Ethernet port on the management station to the LAN Port of the Firewall.

3 Switch on the Firewall.

To do this, connect the power adapter to the port on the back labeled Power.

4 Wait for the Power LED to stop flashing. This takes approximately 90 seconds.

5 Follow the initial configuration steps as described in Chapter 3.

6 Disconnect the management station from the Firewall and reconnect it to the main Ethernet network.

In some cases, you may have to restart the management station after reconnecting it.

7 Attach the Firewall to the LAN (see Chapter 3) and continue with configuration.

12 TROUBLESHOOTING GUIDE

This chapter contains the following:

- Introduction
- Potential Problems and Solutions
- Troubleshooting the Firewall VPN Client
- Frequently Asked Questions about PPPoE

Introduction

The Firewall has been designed to help you detect and solve possible problems with its installation and operation in your network. If you cannot find the solution to the problem in this chapter, please contact Technical Support (see Appendix A for information about contacting Technical Support).

First, try the following:

- Make sure that all equipment is switched on.
- Switch off the Firewall, wait approximately 5 seconds, and then switch it back on. Wait for the Power LED to stop flashing (approximately 90 seconds).

CAUTION: *The contents of the log are lost when resetting the Firewall. If you are trying to diagnose a repeating problem examine the log before resetting the Firewall.*

Potential Problems and Solutions

The following is a list of problems you may experience with your Firewall with some suggested solutions.

Power LED Not Lit

Check if the power cord is plugged into a live power socket.

Power LED Flashes Continuously

If the Power LED continues to flash after 120 seconds, please contact Technical Support (see Appendix A for information about contacting Technical Support).

Power and Alert LED Lit Continuously

If the Power and Alert LEDS are both continuously lit, please contact Technical Support (see Appendix A for information about contacting Technical Support).

Link LED is Off

If the Link LED is not lit, try the following:

- Make sure the Firewall is powered on.
- Make sure the RJ-45 connections are secure. Gently moving the cable back and forth should not make the Link LED turn on and off.
- Make sure the wiring follows the CAT-5 specification. See "Pinout Diagrams" on page 187 for more information.
- Try replacing the cable with a known good cable.
- Try using a standard CAT-5 cable. If the problem is on the LAN or DMZ port, try setting the Uplink/Normal switch to the alternative position.

Ethernet Connection is Not Functioning

If the Ethernet connection does not work, try the following:

- Check the physical connections to make sure they are secure.
- Try replacing the cable with a known good cable.

Cannot Access the Web interface

If the Firewall does not allow users or the administrator to log in to establish an authenticated session, try the following:

- Make sure that the Web browser you are using to access the Web interface is supported by the Firewall. Netscape Navigator 4 or Internet Explorer 4 or higher versions are supported.
- During the initial configuration, make sure that you change the IP address for the management station to one in the same subnet as the Firewall, such as `192.168.1.200`.
- Make sure the Web browser has Java, JavaScript, or ActiveX enabled.
- Make sure the users are attempting to log into the correct IP address. The correct address is the management IP Address of the Firewall, and not the Public Address, if NAT is enabled.
- Make sure that users are attempting to log in with a valid user name and password.

- Remember that passwords are case-sensitive; make sure the Caps Lock key is off.
- Click *Reload* or *Refresh* in the Web browser and try again. For security reasons, the Firewall sends a slightly different Authentication page each time you log in to the Web interface. If the password you use does not allow access to the Firewall, it might be because the browser is displaying a cached copy of the page instead of the current page.
- If you cannot remember the correct password, you can reset the Firewall. See Appendix H, "Resetting the Firewall" for more information.

LAN Users Cannot Access the Internet

If your users cannot access the Internet, try the following:

- If NAT is enabled, make sure the default router address on the LAN Client is set to the Management IP Address of the Firewall.
- If there are any host devices other than the Internet router connected to the WAN port, they are not accessible to users on the LAN.
- To see if the problem is outside the Firewall, disconnect the Firewall and try to access the Internet.
- Try restarting the router and LAN machines.
- If you are using the Internet Firewall with a cable modem, you may need to register the MAC address of the unit with your cable service provider before connecting the Internet Firewall to your network. You can find the MAC address of the Internet Firewall on a label on the underside of the unit.

Firewall Does Not Save Changes

If the Firewall does not save the changes that you make, make sure that you click *Update* before moving to another window or tab, or all changes are lost.

Duplicate IP Address Errors Are Occurring

If there are duplicate IP address errors after you have installed the Firewall:

- Try restarting the router or LAN machines.
- Make sure the LAN is not connected to the WAN port on the Firewall.
- If DHCP is on, make sure no other DHCP servers are on the LAN.

Machines on the WAN Are Not Reachable

Make sure the Intranet settings in the *Advanced* section are correct.

Troubleshooting the Firewall VPN Client

If the Firewall client is unable to negotiate with the Firewall, the Firewall VPN Client Viewer will display detailed error messages. To access the Log Viewer, select and right click on the icon in the Windows Task Bar and then select Log Viewer.

To view Log messages, try to initiate a VPN session, either by attempting to log into the remote Firewall Web interface, or by pinging a machine on the remote network.

The Log Viewer will display any VPN negotiation errors, such as invalid SPIs or invalid keys.

Error Message Explanations

-
  ```
  "New Connection - Initiating IKE Phase 1 (IP
  ADDR=10.0.030)
  New Connection - SENDING...ISAKMP OAK AG
  (SA,KE,NON,ID,VID)
  New connection - message not received! Retransmitting!"
  ```

  This means the VPN client cannot contact the Firewall either because the VPN client is misconfigured, or the Internet Service Provider for either the Firewall or the VPN client does not pass IPSec packets.

-
  ```
  IreIKE:Unable to acquire CAPI provider handle
  ```

  This indicates that the Firewall VPN client did not install properly. Completely uninstall the VPN client, restart your computer, and then reinstall the VPN client to ensure the client software functions correctly. Confirm that any other IPSec VPN clients have been removed before reinstalling the Firewall VPN client.

The IKE Negotiation on the VPN Client

The IKE Negotiation on the VPN Client requires a certain amount of processor time, before the tunnel opens. This usually takes a few seconds to complete and some packets may be lost during the process.

There is no negotiation time when using Manual Keys

Restarting the Firewall with Active VPN Tunnel

If you restart the Firewall with a VPN Client active you must deactivate and reactivate the IRE VPN Client. Restarting the Firewall kills all the current VPN tunnels on the Firewall side. In this case the IRE VPN assumes that the connection is still intact and sends encrypted packets that eventually get dropped.

A easy way to restart the negotiation on the client side is to click on the floppy disk icon at the top of the Security Policy Editor screen.

Export the VPN Client Security Policy File

1 Select *Export Security Policy* in the *File* menu at the top of the *Security Policy Editor* window.

2 Click *Yes* to lock the Security Policy and prevent remote users from changing the VPN client policy. Click *No* to permit remote user configuration. Then name the security policy database file (*.spd) and save it to a local folder or to a floppy disk.

Import the VPN Client Security Policy File

1 Select *Import Security Policy* in the *File* menu at the top of the *Security Policy Editor* window.

2 Browse your local hard drive for the desired security policy database file (*.spd) and click *Open*.

Uninstall the VPN Client

1 To uninstall the Firewall VPN Client, open the *Control Panel* in the Windows *Start* menu.

2 Double click *Add/Remove Programs* in the Control Panel window.

3 Select *IRE VPN Client* in the Add/Remove Programs Properties window and click *Add/Remove*.

4 Click *Yes* in the Confirm File Deletion window to delete the VPN client and all of its components.

5 Click *Yes* to save the security policy database file to the Firewall VPN Client.

Frequently Asked Questions about PPPoE

Why are ISPs using PPPoE in their broadband services?

The theory is that PPPoE makes it easier for the end user of broadband services to connect to the Internet by simulating a Dial-up connection. The ISP realizes significant advantages because much of the existing Dial-up infrastructure (billing, authentication, security, etc.) can be used for DSL and other broadband services.

How do you connect to the Internet using PPPoE?

Along with a broadband modem, the ISP will install a software application on your computer that asks for a username and password. After this information is provided, the connection is established allowing the user to access the Internet.

What are some problems with PPPoE?

- Multiple accounts — The biggest problem using PPPoE without a Firewall is that the ISP requires the customer to have a PPPoE account for each computer attempting to access the Internet. The Firewall is able to manage PPPoE connections eliminating the need to install PPPoE software on each client machine.
- Home networking — Many home networking products don't support PPPoE, and if they do, configuration can be increasingly complex.
- Performance — There can also be a decrease in performance caused by the overhead required by PPPoE. In addition to sending the data and the Ethernet addresses and routing information, the PPPoE information must also be sent, adding to the overall bandwidth required for the transmission.

Can I have one PPPoE account for multiple computers in my home?

Yes. Using the PPPoE firmware, it is possible to have multiple computers share a single account from your service provider. This can save time and money in the set up and monthly fees of multiple PPPoE accounts.

IV Firewall and Networking Concepts

Chapter 13 Types of Attack and Firewall Defences

Chapter 14 Networking Concepts

13 Types of Attack and Firewall Defences

This chapter describes the some of attacks that hackers may use to infiltrate and attack your network. It also details the way in which the Firewall will counter the attacks. The following sections are covered in this chapter:

- Denial of Service Attacks
- Intrusion Attacks
- Trojan Horse Attacks

Denial of Service Attacks

Denial of Service (DoS) attacks are malicious attacks designed to cause harm. The consequences of an attack range from the loss of few seconds of time on a web server or network to the crash of a server. In the worst case the attacker can learn enough about your company infrastructure and exploit its vulnerabilities to crash any server at will.

Denial of Service attacks work by exploiting weaknesses in TCP/IP, exploiting weaknesses in your servers or by generating large amounts of traffic (brute force attacks). Commonly attempted attacks and the reaction of the SuperStack® 3 Firewall are listed below.

Ping of Death

A *ping of death* attack attempts to crash your system by sending a fragmented packet which, when reconstructed is larger than the maximum allowable size. Other known variants of the *ping of death* include *teardrop*, *bonk* and *nestea.*

Firewall Response: Packet is dropped. Attack is stopped.

Smurf Attack

A *smurf attack* involves two systems. The attacker sends a packet containing a ICMP echo request (ping) to the network address of one system. This system is known as the amplifier.

The return address of the ping has been faked (spoofed) to appear to come from a machine on another network (the victim). The victim is then flooded with responses to the ping. As many responses are generated for only one attack, the attacker is able use many amplifiers on the same victim.

The results of a *smurf attack* range from slowing of the network to the crashing of the victim devices.

Firewall Response as Amplifier: Spoofed IP address is detected and packet is dropped. Firewall will not act as amplifier.

Firewall Response as Victim: Traffic from a *smurf attack* cannot be separated from other network traffic. Traffic is allowed to pass.

SYN Flood Attack

A *SYN flood attack* attempts to slow your network by requesting new connections but not completing the process to open the connection. Once the buffer for these pending connections is full a server will not accept any more connections and will be unresponsive.

Firewall Response: The connection request will be completed by the Firewall and the connection monitored to check if data is sent. If no data is sent the Firewall resets the connection.

Land Attack

A *land attack* is an attempt to slow your network down by sending a packet with identical source and destination addresses originating from your network.

Firewall Response: Packet is dropped. Attack is stopped.

Intrusion Attacks

An *Intrusion Attack* is designed to get information from your network or place information on your network. This may be the theft of confidential material, the defacing of a web site or the theft of passwords or discovery of network infrastructure that will enable further attacks.

External Access

Without a firewall your network can be accessed from anywhere on the *Wide Area Network* (WAN) outside your network. The Firewall blocks all attempts to access the *Local Area Network* (LAN) that are initiated from outside your network

Firewall response: Packet is dropped. Attack is stopped.

Port Scanning

Port Scanning is the testing of ports to see which are active and which are disabled. Although ports are scanned as part of normal traffic the scanning of many ports in a short period of time is a common precursor to an attack

Firewall Response: None - the Firewall will allow *port scanning* but will log all port scans to aid diagnosis. Ports not in use will be disabled by the Firewall.

IP Spoofing

IP Spoofing is a method of masking the identity of an intrusion by making it appear that the traffic came from a different computer. This is used by intruders to keep their anonymity and can be used in a *Denial of Service* attack.

Firewall Response: The Firewall will drop any spoofed packets log the event and alert the administrator.

Trojan Horse Attacks

Trojan Horse attacks rely on a piece of software installed within your network prior to the attack. Attacks vary in severity and effect from showing messages on screen or crashing an individual PC to theft of information and infiltration of the network.

The *Firewall* blocks attacks in two ways:

- Known *Trojan Horse* attacks are identified and blocked.
- Ports not in use are blocked by default.

Trojan Horse attacks that the firewall is capable of blocking include: Back Orifice, ini killer, *NetBus*, *NetSpy*, *Priority*, *Ripper*, *Senna Spy*, *Striker,* and *SubSeven*.

Using an anti-virus tool and updating the firmware of your Firewall as soon as a new version is available will significantly increase your chance of resisting a Trojan Horse attack.

14 NETWORKING CONCEPTS

This appendix contains the following:

- Introduction to TCP/IP
- Network Address Translation (NAT)
- Dynamic Host Configuration Protocol (DHCP)
- Port Numbers
- Virtual Private Network Services

Introduction to TCP/IP

Protocols are rules that networking hardware and software follow to communicate with one another. The Firewall uses the TCP/IP protocol.

IP and TCP

IP stands for Internet Protocol. This protocol provides connectionless data transfer over a TCP/IP network. Because IP alone does not provide end-to-end data reliability as well as some other services, other protocols such as TCP can be added to provide these services. TCP stands for Transmission Control Protocol. In TCP/IP, TCP works with IP to ensure the integrity of the data traveling over the network. TCP/IP is the protocol of the Internet.

IP Addressing

To become part of an IP network, a network device must have an IP address. An IP address is a unique number that differentiates one device from another on the network to avoid confusion during communication. To help illustrate IP addresses, the following sections compare an IP address to the telephone numbering system, a system that is used every day.

Like a phone number with a long distance number and area code, an IP address contains a set of four numbers. Where the components in phone numbers can be separated with dashes, for example, `1-408-555-1212`, IP address number components are separated by decimal points or dots (called *dotted decimal notation*), for example, `123.45.67.89`. Because computers use a binary number system, each number in the set must be less than 255.

There are three components that contribute to an IP address:

- IP address itself
- Subnet mask
- Default gateway

The following sections discuss each of these components in detail.

IP Address

Just as each household or business requires a unique phone number, a networked device (such as a computer, printer, file server, or router) must have a unique IP address. Unlike phone numbers, in IP addressing it is necessary to always use the entire number when communicating with other devices.

There are three classes of IP addresses: A, B, and C. Like a main business phone number that one can call and then be transferred through interchange numbers to an individual's extension number, the different classes of IP addresses provide for varying levels of *interchanges* or subnetworks and *extensions* or device numbers. The classes are based on estimated network size:

- Class A — used for very large networks with hundreds of subnetworks and thousands of devices. Class A networks use IP addresses between `0.0.0.0` and `127.0.0.0`.
- Class B — used for medium to large networks with 10–100 subnetworks and hundreds of devices. Class B networks use IP addresses between `128.0.0.0` and `191.0.0.0`.
- Class C — used for small to medium networks, usually with only a few subnetworks and less than 200 devices. Class C networks use IP addresses between `192.0.0.0` and `223.0.0.0`.

Just as you obtain a phone number from the phone company, there are controlling bodies for IP addresses. The overall controlling body for IP addresses worldwide is InterNIC. Businesses or individuals can request one or many IP addresses from InterNIC; if you can estimate the future growth of the network, this can help you to work out the class and number of IP addresses you need.

Most large centralized companies have a network manager in charge of all IP address numbers. Other companies have a distributed administration scheme that allows the local network manager to set local IP addresses. In this case, the local manager gets a sub network or "interchange" number from the company's central network manager and then assigns local IP address numbers.

Subnet Mask

As mentioned in "IP Address" on page 180, the IP addressing system allows creation of subnetworks or *interchanges* and device numbers or *extensions* within those subnetworks. These numbers are created using a mathematical device called a subnet mask. A subnet mask, like the IP address, is a set of four numbers in dotted decimal notation. Subnet masks typically take three forms:

- `255.0.0.0`
- `255.255.0.0`
- `255.255.255.0`

The number 255 *masks* out the corresponding number of the IP address, resulting in IP address numbers that are valid for the network. For example, an IP address of `123.45.67.89` and a subnet mask of `255.255.255.0` results in a sub network number of `123.45.67.0` and a device number of `89`. The IP address numbers that are valid to use are those assigned by InterNIC; this prevents someone setting up IP addresses that are duplicates of those at another company.

The subnet mask used for the network typically corresponds to the class of IP address assigned. If the IP address is Class A, use a subnet mask of `255.0.0.0`. Class B addresses use a subnet mask of `255.255.0.0`, and Class C IP addresses use a subnet mask of `255.255.255.0`.

Default Gateway

A default gateway is like a long distance operator — users can dial the operator to get assistance connecting to the end party. In complex networks with many subnetworks, gateways keep traffic from traveling between different subnetworks unless addressed to travel there. While this helps to keep overall network traffic more manageable, it also introduces another level of complexity.

To communicate with a device on another network, the message must go through a gateway that connects the two networks. Therefore, users need to know the default gateway's IP address. If there is no gateway in the network, use an IP address of `0.0.0.0` in fields that apply to a default gateway.

Network Address Translation (NAT)

Network Address Translation (NAT) is used to re-map all the addresses on a LAN to a single address on the Internet. This can be useful for three reasons:

- You may have a pre-existing LAN, not connected to the Internet, which uses invalid Internet addresses. NAT can be used to connect these machines to the Internet without changing all of their addresses.
- You may wish to obtain a single-user account from your Internet Service Provider instead of a LAN account, since single user accounts tend to be cheaper. NAT can be used to make all the machines on your LAN appear to be a single computer hooked up to the Internet.
- Additional security is provided when all the addresses on your network are invisible to the outside world.

If you wish to use addresses on your LAN, which have not been assigned to you by your Internet Service Provider, it is a good idea to use addresses in a special range allocated for this purpose. The following three blocks of IP address space have been reserved by the Internet Assigned Numbers Authority for the purpose of creating private internets:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

If you use some other arbitrary range, then there is the chance that the range is actually in use by someone else on the Internet. If this is the case, you will not be able to access their sites from your LAN.

If you reconfigure the IP addresses of the machines on your LAN, it is sometimes necessary to change their Default Gateway address as well.

Limitations of Using NAT

- NAT and Remote Access are not compatible features, since NAT hides machines on your LAN from the Internet. If NAT is on, the only machines on the LAN, which can be accessed, are those designated as “Public LAN Servers”; these are available to anonymous users on the Internet without authentication.

- Not All Applications lend themselves easily to address translation by NAT devices. Especially, the applications that carry IP Addresses inside the payload.
- NAT devices operate on the assumption that each session is independent. Application, such as H.323, that use one or more control follow-on sessions, require the use of an Application Level Gateway (ALG). The ALG will help interpret and translate the payload, so that it will be prepared for follow-on data sessions.
- NAT increases the risk of mis-addressing. For example, the same local address may be bound to different global address at different times and vise versa.

For more information on NAT, see
`http://www.ietf.org/rfc/rfc2663.txt`

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol is a protocol that allows computers on a network to get TCP/IP settings from a centralized server. This configuration information includes elements such as IP Address, subnet mask, DNS server address, and so forth. Here's how it works:

A DHCP server provides a dynamic, “leased” address to a DHCP client. This means that the client will be able to use the provided IP address for a certain period of time. The DHCP server will not give this address to a different client during the lease period, thus ensuring that there are no address conflicts. When the lease expires, then the client may renew the lease. If it does not renew the lease (for instance, if it has been switched off), then the server may give the dynamic address to a different client.

The Firewall contains both a DHCP server and client. They are used for different purposes. The DHCP server can be used to provide machines on the LAN with configuration information. This can make it much easier to administer these machines, since individual hosts do not need to configure one-at-a-time. The Firewall's DHCP server also supports an older protocol called “BootP”.

The DHCP client is used in conjunction with Network Address Translation. The Firewall can use its DHCP client to automatically configure the Firewall WAN IP Address, WAN subnet mask, and other parameters. This can be useful for corporate Intranets, cable modem networks, or other environments where dynamic addressing is desirable.

Port Numbers

The port numbers are divided into three ranges:

- Well Known ports — those from 0 to 1023
- Registered ports — those from 1024 to 49151
- Dynamic or Private ports — those from 49152 to 65535

Well Known Port Numbers

The Well Known Ports are controlled and assigned by the Internet Assigned Numbers Authority (IANA) **`http://www.iana.org`** and on most systems can only be used by system processes, or by programs executed by privileged users. Many popular services, such as Web, FTP, SMTP/POP3 e-mail, DNS and so forth operate in this range.

The assigned ports use a small portion of the possible port numbers. For many years the assigned ports were in the range 0–255. Recently, the range for the assigned ports managed by the IANA has been expanded to the range 0–1023.

Registered Port Numbers

The Registered Ports are not controlled by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users.

While the IANA cannot control uses of these ports, it does list uses of these ports as convenience.

The Registered Ports are in the range 1024–49151.

Visit **`http://www.ietf.org/rfc/rfc1700.txt`** for a list of IP port numbers.

Private Port Numbers

The Private Ports are not controlled or recorded by the IANA and are used in the development of new software and in bespoke programs which will be used by few users only.

The Private Ports are in the range 49152–65535.

Virtual Private Network Services

This section contains the following:

- Introduction to Virtual Private Networks
- VPN Applications

- Basic Terms and Concepts

Introduction to Virtual Private Networks

Virtual Private Networks (VPN) provide an easy, affordable, and secure means for businesses to conduct operations and provide network connectivity to all offices and partners. Using 3Com's intuitive Web interface, a secure connection may be established between two or more sites.

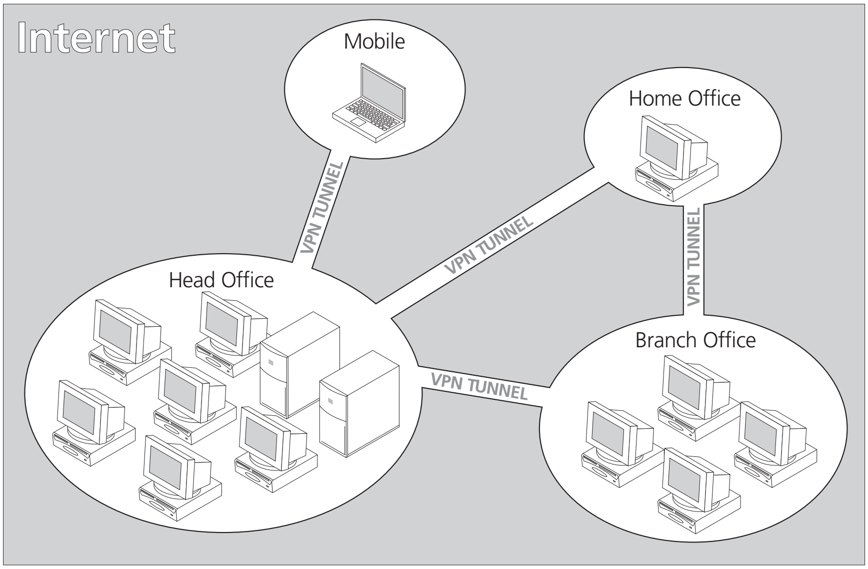
Data that is intended for delivery to a remotely connected site is automatically encrypted using the VPN's accelerated cryptographic processor. The data is delivered via the Web and decrypted at the intended destination.

The SuperStack 3 Firewall VPN implementation uses the IPSec VPN standard. This guarantees compliance with other VPN products, such as 3Com PathBuilder 400 and Check Point Firewall-1 that adhere to the same standard.

VPN Applications

The following illustration shows the VPN connections between the offices and users of a simple company. In this example all external connections are made using VPN tunnels across the Internet.

Figure 65 Virtual Private Networks Applications



- *Linking two or more Private Networks Together*

  VPN is the perfect way to connect branch offices and business partners to the primary business. Using VPN over the Internet, instead of leased site-site lines, offers significant cost savings and improved performance.

- *Using the IRE VPN Client for Secure Remote Management*

  Using the included IRE VPN client for Windows, a secure, encrypted tunnel may be created that allows the administrator to remotely manage the Firewall over the Internet.

- *Accessing Machines Using Private Addressing behind NAT*

  When NAT (Network Address Translation) is enabled, remote users are not able to access hosts on the LAN unless the host is designated a Public LAN Server for that specific protocol. Since the VPN Tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

Basic VPN Terms and Concepts

The following explains the most common terms and expressions used in VPN

- *VPN Tunnel*

  Tunnelling is the encapsulation of point-point transmission inside IP packets. A VPN Tunnel is a term that is used to describe a connection between two or more private nodes or LANs over a public network, typically the Internet. Encryption is often used to maintain the confidentiality of private data when travelling over the Internet.

- *Encryption*

  Encryption is a mathematical operation that transforms data from “clear text” (something that a human or a program can interpret) to “cipher text” (something that cannot be interpreted). Usually the mathematical operation requires that an alphanumeric “key” be supplied along with the clear text. The key and clear text are processed by the encryption operation which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is the mathematical operation that transforms cipher text to clear text. Decryption also requires a key.

- *Key*

  A key is an alphanumeric string that is used by the encryption operation to transform clear text into cipher text. Keys used in VPN communications can range in length, but are typically 16 or 32 characters. The longer the key, the more difficult it is to break the encryption. The reason for this is most methods used to break encryption involve trying every possible combination of characters, similar to trying to open a safe when the combination is not known.

- *Asymmetric vs. Symmetric Cryptography*

  Asymmetric and symmetric cryptography refer to the keys used to authenticate, or encrypt and decrypt the data.

  Asymmetric cryptography does not use the same key to verify the data. Asymmetric cryptography is often referred to as public key cryptography. With public key, each user gets a pair of keys, one called the public key and the other called the private key. The private key is always linked mathematically to the public key to be kept secret. All communications involve only public keys; the private key is never transmitted or shared, but used to decrypt the message. A user can generate their own keys using key generation software, or have keys generated by trusted organizations. Once a key has been generated, the user must register his or her public key with a central administration, called a Certifying Authority (CA). Organizations, such as RSA Data Security and Verisign, can help users issue and register key pairs.

  The Firewall VPN uses Symmetric Cryptography. As a result, the key on both ends of the VPN tunnel must match exactly.

- *Authentication Header (AH)*

  The Authentication Header is a mechanism for providing strong integrity and authentication for IP packets. Confidentiality and protection from traffic analysis are not provided by the Authentication Header.

  The IP Authentication Header provides security by adding authentication information to an IP packet. This authentication information is calculated using all header and payload data in the IP packet. This provides significantly more security that is currently present in IP.

  Use of AH will increase the processing requirements in the Firewall and will also increase the communication latency. The increased latency is primarily due to the calculation and comparison of the authentication data by the receiver for each IP packet containing an Authentication Header.

- *Data Encryption Standard (DES)*

When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a message authentication code. 3Com's implementation of DES uses a 56-bit key.

3Com's DES Key must be exactly 16 characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f.

- *Strong Encryption (Triple DES or 3DES)*

  Strong Encryption, or Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is dramatically more secure that DES, and is considered to be virtually unbreakable by security experts. It also requires a great deal more processing power, resulting in increased latency and decreased throughput.

  The 3DES Key must be exactly 24 characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f.

- *ARCFour*

  ARCFour (ARC4) is used for communications with secure Web Sites using the SSL protocol. Many banks use a 40-bit key ARC4 for online banking while others use a 128-bit key. 3Com's implementation of ARCFour uses a 56-bit key.

  ARCFour is faster than DES for several reasons. First is that it is a newer encryption mechanism than DES. As a result, it benefits from advances in encryption technology. Second, unlike DES, it is designed to encrypt data streams, rather than static storage. DES has achieved much of its popularity because it is well known and has been proven to be very robust. ARCFour, while theoretically as secure as 56bit DES, does not have the long history that leads to the wide acceptance by security professionals.

  3Com's ARCFour Key must be exactly 16 characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f.

- *Security Parameter Index (SPI)*

  The SPI is used to establish a VPN tunnel. The SPI is transmitted from the remote Firewall to the local Firewall. The local Firewall then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

The SPI must be unique, is from one to eight characters long, and is comprised of hexadecimal characters. Valid hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f.

The range from "0" to "ff" inclusive, is reserved by the Internet Engineering Task Force (IETF) and are not allowed for use as an SPI. They will not be accepted by the Firewall when entered as an SPI; an error message will be displayed at the bottom of the Web browser window when the Update button is pressed.

- *Security Association (SA)*

  A Security Association is the group of security settings relating to a given network connection or set of connections. The Security Association is based on the SPI, and includes the Destination Address Range, IPSec gateway Address, Encryption method, Encryption Key and Authentication Key.

V APPENDICES

A Safety Information

***WARNING**: Please read the ‘Important Safety Information’ section before you start.*

***VORSICHT**: Bitte lesen Sie den Abschnitt ‘Wichtige Sicherheitsinformationen’ sorgfältig durch, bevor Sie das Gerät einschalten.*

***AVERTISSEMENT**: Veuillez lire attentivement la section ‘Consignes importantes de sécurité’ avant de mettre en route.*

Important Safety Information

***WARNING:** Warnings contain directions that you must follow for your personal safety. Follow all directions carefully.*
You must read the following safety information carefully before you install or remove the unit:

***WARNING**: Exceptional care must be taken during installation and removal of the unit.*

***WARNING**: To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.*

***WARNING**: The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.*

***WARNING**: This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.*

WARNING*: There are no user-replaceable fuses or user-serviceable parts inside the unit. If you have a physical problem with the unit that cannot be solved with problem solving actions in this guide, contact your supplier.*

WARNING*: Disconnect the power adapter before moving the unit.*

WARNING: *RJ-45 Ports. These are shielded RJ-45 data sockets. They cannot be used as standard traditional telephone sockets, or to connect the unit to a traditional PBX or public telephone network. Only connect RJ-45 data connectors, network telephony systems, or network telephones to these sockets. Either shielded or unshielded data cables with shielded or unshielded jacks can be connected to these data sockets.*

Wichtige Sicherheitshinweise

VORSICHT: *Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen.*

VORSICHT: *Sie müssen die folgenden Sicherheitsinformationen sorgfältig durchlesen, bevor Sie das Gerät installieren oder ausbauen:*

VORSICHT: *Bei der Installation und beim Ausbau des Geräts ist mit höchster Vorsicht vorzugehen.*

VORSICHT: *Stapeln Sie das Gerät nur mit anderen SuperStack 3 Gerätes zusammen.*

VORSICHT: *Aufgrund von internationalen Sicherheitsnormen darf das Gerät nur mit dem mitgelieferten Netzadapter verwendet werden.*

VORSICHT: *Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.*

VORSICHT: *Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.*

VORSICHT: *Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Switch haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.*

VORSICHT: *Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.*

VORSICHT: *RJ-45-Porte. Diese Porte sind geschützte Dat-ensteckdosen. Sie dürfen weder wie normale traditionelle Tele-fonsteckdosen noch für die Verbindung der Einheit mit einem traditionellem privatem oder öffentlichem Telefonnetzwerk gebraucht werden. Nur RJ-45-Datenanscluße, Telefonnetzsysteme or Netztelefone an diese Steckdosen anschließen.*

Entweder geschützte oder ungeschützte Buchsen dürfen an diese Datensteckdosen angeschlossen werden.

Consignes Importantes de Sécurité

AVERTISSEMENT: *Les avertissements présentent des consignes que vous devez respecter pour garantir votre sécurité personnelle. Vous devez respecter attentivement toutes les consignes.*

Nous vous demandons de lire attentivement les consignes suivantes de sécurité avant d'installer ou de retirer l'appareil:

AVERTISSEMENT: *Faites très attention lors de l'installation et de la dépose du groupe.*

AVERTISSEMENT: *Seulement entasser le moyer avec les autres moyeux SuperStack 3.*

AVERTISSEMENT: *Pour garantir le respect des normes internationales de sécurité, utilisez uniquement l'adaptateur électrique remis avec cet appareil.*

AVERTISSEMENT: *La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.*

AVERTISSEMENT: *L’appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.*

AVERTISSEMENT: *Il n’y a pas de parties remplaceables par les utilisateurs ou entretenues par les utilisateurs à l’intérieur du moyeu. Si vous avez un problème physique avec le moyeu qui ne peut pas être résolu avec les actions de la résolution des problèmes dans ce guide, contacter votre fournisseur.*

AVERTISSEMENT: *Débranchez l'adaptateur électrique avant de retirer cet appareil.*

AVERTISSEMENT: *Points d’accès RJ-45. Ceux-ci sont protégés par des prises de données. Ils ne peuvent pas être utilisés comme prises de téléphone conventionnelles standard, ni pour la connection de l’unité à un réseau téléphonique central privé ou public. Raccorder seulement connecteurs de données RJ-45, systèmes de réseaux de téléphonie ou téléphones de réseaux à ces prises.*
Il est possible de raccorder des câbles protégés ou non protégés avec des jacks protégés ou non protégés à ces prises de données.

B

Technical Specifications and Standards

This appendix lists the technical specifications for the SuperStack 3 Firewall. The Firewall has been designed and certified to the following standards:

Table 7 Technical Specifications of the Firewall

Physical
Width: 440 mm (17.3 in.)
Depth: 230 mm (9.0 in.)
Height: 44 mm (1.7 in.) or 1 U
Weight: 2.55 kg (5.6 lb)
Mounting: Free standing, or 19in. rack mounting using the mounting kit supplied
Capacity
Maximum Number of Simultaneous IP Connections: 30,000
Maximum Number of Security Associations: 1,000
Maximum Number of VPN Tunnels: 1,999
Size of DHCP pool: 255 bindings
Maximum Number of Rules: 100
Maximum Number of Custom Rules: 64
AC Line Frequency
50-60Hz
Current Rating (max): 3.15A
Input Voltage: 90–264Vrms
Operating Temperature
0–50 °C (32–122 °F)
Humidity
10–95% (non-condensing)
Electrical Interfaces
Three 10/100 BASE-T RJ45 Connectors

Table 7 Technical Specifications of the Firewall

Functional
ISO/IEC 8802-3, IEEE 802.3, ICSA Firewall Certification
Safety
UL1950, EN 60950, CSA 22.2 #950, IEC 950
EMC
EN55022 Class A, EN 50082-1, FCC Part 15 Part Class A, ICES-003 Class A, VCCI Class A, EN 55024, CNS 13438 Class A
Environmental
EN 60068 (IEC 68)
Power Inlet
IEC 320

C CABLE SPECIFICATIONS

Cable Specifications

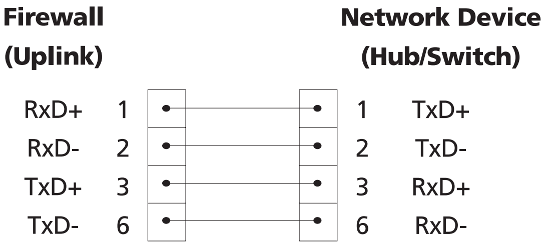
The Firewall supports the following cable types and maximum lengths:

- Category 5 cable.
- Maximum cable length of 100 m (327.86 ft).

Pinout Diagrams

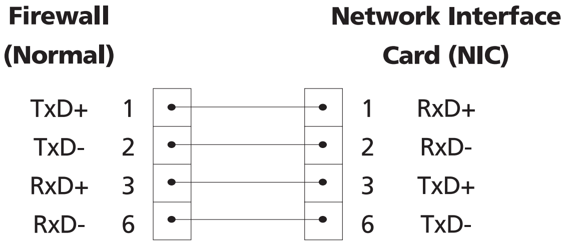
Figure 66 and Figure 67 below show the pin connections when using a straight through Category 5 cable. This is the standard cable used for Ethernet and Fast Ethernet.

Figure 66 Connecting the Firewall to a hub or switch using a straight through cable



Pins 4, 5, 7 and 8 are not used

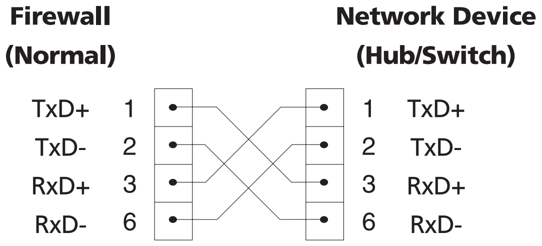
Figure 67 Connecting the Firewall to a Network Interface Card using a straight through cable



Pins 4, 5, 7 and 8 are not used

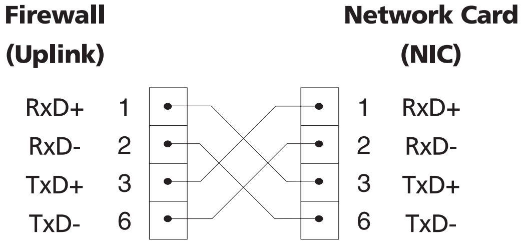
Figure 68 and Figure 69 below show the pin connections when using a crossover Category 5 cable. It is not necessary to use a crossover cable with your Firewall as the Normal/Uplink switch beside each port serves the same purpose.

Figure 68 Connecting the firewall to a hub or switch using a crossover cable



Pins 4, 5, 7 and 8 are not used

Figure 69 Connecting the firewall to a network interface card using a crossover cable



Pins 4, 5, 7 and 8 are not used

D TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the most recent information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Knowledgebase Web Services
- 3Com FTP site

World Wide Web Site

To access the latest networking information on the 3Com Corporation World Wide Web site, enter this URL into your Internet browser:

```
http://www.3com.com/
```

This service provides access to online support information such as technical documentation and software, as well as support options that range from technical education to maintenance and professional services.

3Com Knowledgebase Web Services

The 3Com Knowledgebase is a database of technical information to help you install, upgrade, configure, or support 3Com products. The Knowledgebase is updated daily with technical information discovered by 3Com technical support engineers. This complimentary service, which is available 24 hours a day, 7 days a week to 3Com customers and partners, is located on the 3Com Corporation World Wide Web site at:

```
http://knowledgebase.3com.com
```

3Com FTP Site

Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **`ftp.3com.com`**
- Username: **`anonymous`**
- Password: **`<your Internet e-mail address>`**

ℹ *You do not need a user name and password with Web browser software such as Netscape Navigator and Internet Explorer.*

Support from Your Network Supplier

If you require additional assistance, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, call the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number

- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Here is a list of worldwide technical telephone support numbers. These numbers are correct at the time of publication. Refer to the 3Com Web site for updated information.

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim			
Australia	1 800 678 515	P.R. of China	10800 61 00137 or
Hong Kong	800 933 486		021 6350 1590 or
India	+61 2 9937 5085 or		00800 0638 3266
	000800 6501111	Singapore	800 6161 463
Indonesia	001 800 61 009	S. Korea	00798 611 2230 or
Japan	03 5783 1270		02 3455 6455
Malaysia	1800 801 777	Taiwan, R.O.C.	00798 611 2230
New Zealand	0800 446 398	Thailand	0080 611 261
Pakistan	+61 2 9937 5083		001 800 611 2000
Philippines	1235 61 266 2602		
Europe, Middle East and Africa			
From anywhere in these regions, call:	+44 (0)1442 435529 phone +44 (0)1442 432524 fax		
Europe and South Africa From the following countries, you may use the toll-free numbers:			
Austria	0800 297468	Luxembourg	0800 3625
Belgium	0800 71429	Netherlands	0800 0227788
Denmark	800 17309	Norway	800 11376
Finland	0800 113153	Poland	00800 3111206
France	0800 917959	Portugal	0800 831416
Germany	0800 1821502	South Africa	0800 995014
Hungary	06800 12813	Spain	900 983125
Ireland	1800 553117	Sweden	020 795482
Israel	1800 9453794	Switzerland	0800 55 3072
Italy	800 8 79489	U.K.	0800 966197
Latin America			
Brazil	0800 13 3266	Puerto Rico	800 666 5065
Mexico	01 800 849CARE	Central and South America	AT&T +800 998 2112
North America	1 800 NET 3Com (1 800 638 3266)		
	Enterprise Customers: 1 800 876-3266		

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain an authorization number. Products sent to 3Com without authorization numbers will be returned to the sender unopened, at the sender's expense.

To obtain an authorization number, call or fax:

Country	Telephone Number	Fax Number
Asia, Pacific Rim	+ 65 543 6500	+ 65 543 6348
Europe, South Africa, and Middle East	+44 (0)1442 435529	+ 44 (0)1442 432524
Central and South America	525 201 0075	
Argentina	0810 222 3266	
Bolivia	511 241 1691	
Brazil	0800 133266 or 55 11 5643 2700	
Caribbean	525 201 0004	
Chile	562 240 6200	
Colombia	525 201 0004	
Ecuador	525 201 0004	
Mexico	525 201 0004	
Paraguay	525 201 0004	
Peru	511 241 1691	
Uruguay	525 201 0004	
Venezuela	525 201 0004	
From the following countries, you may call the toll-free numbers; select option 2 and then option 2:		
Austria	0800 297468	
Belgium	0800 71429	
Denmark	800 17309	
Finland	0800 113153	
France	0800 917959	
Germany	0800 1821502	
Hungary	00800 12813	
Ireland	1800553117	
Israel	1800 9453794	
Italy	1678 79489	
Netherlands	0800 0227788	
Norway	800 11376	
Poland	00800 3111206	
Portugal	0800 831416	
South Africa	0800 995014	
Spain	900 983125	
Sweden	020 795482	
Switzerland	0800 55 3072	
U.K.	0800 966197	

Country	Telephone Number	Fax Number
U.S.A. and Canada	1 800 NET 3Com (1 800 638 3266) Enterprise Customers: 1 800 876 3266	1 408 326 7120 (not toll-free)

INDEX

REGULATORY NOTICES

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference to radio communications, in which case the user will be required to correct the interference at their own expense.

INFORMATION TO THE USER

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

CSA STATEMENT

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

CE STATEMENT (EUROPE)

This product complies with the European Low Voltage Directive 73/23/EEC and EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC.

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

VCCI STATEMENT

　この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI STATEMENT

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。